



Release Notes for Avaya Ethernet Routing Switch 4800 Series

Release 5.10
NN47205-400
Issue 14.09
March 2018

© 2014-2017, Avaya Inc.
All Rights Reserved.

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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/LicenseInfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

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

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE

AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(s) 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.

Contents

Chapter 1: Introduction	7
Purpose.....	7
Chapter 2: New in this release	8
Features.....	8
Ability to query USB file information.....	8
ACLI pipe filter commands.....	8
AUR and AAUR enhancement.....	8
Bi-directional SFP + support.....	9
Disable SSH Client and Telnet Out access.....	9
EAP enhancements.....	10
Enhanced Secure Mode.....	12
E-Tree and Private VLANs.....	13
Fabric Attach enhancements.....	13
MLD Proxy.....	14
Password complexity and password aging and lockout policy.....	15
SHA-2 support for SSH and SSL certificates.....	16
PoE high inrush mode.....	16
RSPAN over MLT/LACP.....	17
SFP DDI information.....	17
SPBM IPv4 Shortcuts	18
Other changes.....	19
Chapter 3: Important notices	20
Supported software and hardware capabilities.....	20
Filter, meter and counter resources.....	23
File names for this release.....	24
Supported traps and notifications.....	25
Tested browsers.....	25
Software upgrade.....	25
Upgrading the software.....	27
Updating switch software.....	31
General software upgrade instructions.....	31
Changing switch software in ACLI.....	31
Job aid—download command parameters.....	32
Changing switch software in EDM.....	33
Job aid—File System screen fields.....	34
Setting IP parameters with the ip.cfg file on a USB memory device.....	36
Hardware and software compatibility.....	38
XFP, SFP and SFP+ Transceiver Compatibility.....	38
Supported standards, RFCs and MIBs.....	43

Contents

Standards.....	43
RFCs.....	44
IPv6 specific RFCs.....	48
Chapter 4: Resolved issues	50
Chapter 5: Known issues and limitations	51
Known issues and limitations for Release 5.10.....	51
IPv6 limitations.....	53
Chapter 6: Resources	55
Support.....	55
Searching a documentation collection.....	56
Subscribing to e-notifications.....	57

Chapter 1: Introduction

Purpose

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Avaya Ethernet Routing Switch 4800 Series, Software Release 5.10.

 **Note:**

Release 5.10 is supported only on ERS 4800 series.

Chapter 2: New in this release

The following sections detail what is new in *Release Notes for Avaya Ethernet Routing Switch 4800 Series* in this release.

Features

See the following sections for information about the new features in this release.

Ability to query USB file information

General information about the files on a USB flash device can be viewed in Enterprise Device Manager.

For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series, NN47205-102*.

ACLI pipe filter commands

Pipe (|) is used to display only a subset of information in the command output. To filter the command output, type the existing ACLI command followed by the pipe (|) symbol and then, the pipe filter command. The output contains only the lines specified in the pipe filter.

For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series, NN47205-102*.

AUR and AAUR enhancement

Auto Unit Replacement (AUR) and Agent Auto Unit Replacement (AAUR) features are enhanced to support base unit replacement for a stack of two switches.

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series, NN47205-500*.

Ensure to check the following while replacing a unit or base unit in the stack:

- The new unit must be the same hardware configuration as the old, including the same number of ports.
- If a new unit is added with a different hardware configuration, the stored configuration of the unit being replaced is not loaded on the new unit.
- If a new unit is added with the same hardware configuration, the previous configuration of the new unit is lost. The configuration is overwritten with the restored configuration from the stack.
- You can enable or disable this feature at any time using ACLI. The default mode is Enable.
- Match the position of the Base Unit switch to the unit being replaced.

Bi-directional SFP + support

The following 10 Gbps bi-directional transceivers are supported:

- 10GBASE-BX10 SFP+ AA1403169-E6
- 10GBASE-BX10 SFP+ AA1403170-E6

For more information, see *Installing Transceivers and Optical Components on Avaya Ethernet Routing Switch 4800 Series, NN47205-301*.

Disable SSH Client and Telnet Out access

Only the users with Read-Write access can enable or disable the remote access for themselves and for everyone else.

The remote access can be configured to allow users to enable or disable SSH Client and Telnet Out access on a device. The configuration is supported only through ACLI and can be used only on base unit.

If the remote connection is disabled, all open SSH Client or Telnet Out sessions are disabled for all users including the users with Read-Write access. Also, remote access changes done by Read-Write users, propagates to all open sessions on device (console, telnet or SSH).

By default, the remote access is disabled.

Configuring remote connection

About this task

Users with Read-Write access can configure remote access and allow users to enable or disable SSH Client and Telnet Out access on device.

When the remote access is disabled, all users are not allowed to open sessions. Only the users with Read-Write role can enable or disable the remote access for themselves and for everyone else. By default, the remote access is disabled.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable SSH Client and Telnet Out access on a device:

```
remote connection enable
```

3. Display the remote connection status:

```
show remote connection
```

4. **(Optional)** Disable SSH Client and Telnet Out access on a device:

```
remote connection disable
```

Example

Following is an example to enable remote connection:

```
Switch(config)#remote connection enable
% Remote access has been enabled on this device !
```

Following is an example to disable remote connection:

```
Switch(config)#remote connection disable
% Remote access has been disabled on this device !
```

Following is an example to display remote connection status:

```
Switch(config)#show remote connection
% Remote access for this device is: Disabled
Switch(config)#ssh 192.0.2.1
% Remote access is disabled on this device !
Switch(config)#telnet 192.0.2.1
% Remote access is disabled on this device !
% Remote access is disabled on this device !
```

EAP enhancements

See the following sections for information about feature changes.

Configuring RADIUS server reachability

A new CLI command is introduced to trigger RADIUS server reachability instantly without having to wait for periodic checks.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Delayed MAC authentication

The purpose of this feature is to give priority to another means of authentication other than Non-EAP through Radius.

Because of simultaneous EAP and Non-EAP authentication (with Non-EAP being faster), the Delayed MAC Authentication features allows a global delay timer, ranging from 0 to 20 seconds to be configured. When traffic is visible from a MAC, the switch waits the configured delay time before Non-EAP traffic is authenticated through the RADIUS server.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Dual key authentication

VSAs are added to support dual key authentication.

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4800 Series*, NN47205-507.

RADIUS authentication delay

RADIUS authentication delay prevents authentication issues caused by bursts of re-authentication requests sent to the RADIUS Server.

In scalability setups, there are situations when the RADIUS Servers cannot respond to all these requests. Even if the RADIUS Server responds to all re-authentication requests, the switch may be unable to process all of them.

RADIUS authentication delay introduces a delay between authentications when a burst is detected. The switch limits the RADIUS requests it sends to 50 packets per second. The re-authentication period for EAP and NEAP clients is limited to a period of minimum 60 seconds.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

Track all MACs per port

This feature tracks the following information per port:

- EAP and non EAP authentication and non-authenticated clients
- status of the RADIUS server authentication response if the MAC is rejected or is not authenticated

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

RFC4675 RADIUS attributes: Egress-VLANID and Egress-VLAN-NAME

Egress-VLANID and Egress-VLAN-NAME attributes control the 802.1Q tagging for traffic egressing a port where RADIUS authentication was performed for a connected EAP or non-EAP client.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

ACL commands

The following new ACL commands are supported:

- `radius reachability check [eap | non-eap | global]`

- `eapol multihost radius-non-eap-delay [0-20]`
- `show eapol sessions`

The following ACLI commands are obsolete:

- `show eapol multihost status`
- `show eapol multihost non-eap-mac status`

For more information, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 4800 Series*, NN47205-105.

Enhanced Secure Mode

Enhanced secure mode is a boot mode operation. By default, enhanced secure mode is disabled. The switch must be restarted after the feature is enabled or disabled in order to apply the new setting.

Configurations are not transferable between operating modes with enhanced secure mode enabled or enhanced secure mode disabled. The switch resets to default configuration when the modes of operation are switched.

The switch defaults to higher level of security when Enhanced Secure Mode is enabled.

The following security enhancements are available in this operating mode:

- The switch supports multiple role-based access levels.
- Every attempt to access the product requires a username and password to be presented for authentication.
- The switch enforces stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.
- The audit logging is enabled by default and cannot be disabled or modified. The audit records all valid activities performed on the system, including the identity of each user through its username, IP and session ID and the date and time stamp of access attempt. If you configure a remote Syslog server, the switch sends each issued command to this remote server. The log file is not affected by a restart or a default boot. Log encryption is supported.
- The command for configuring the switch banner provides an option to display the DoD approved banner.
- TFTP protocol is disabled by default.
- The switch uses NTP as default clock source. NTP authentication keys are hidden in ACLI and ASCII config.

For more information see, *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

ACLI commands

This feature introduces the following commands:

- `enhanced-secure-mode`
- `show enhanced-secure-mode`
- `tftp-access`
- `banner usg`

The following ACLI commands have different parameters when enhanced secure mode is enabled:

- `username`
- `password`

The following ACLI commands are not supported when enhanced secure mode is enabled:

- `audit log save`
- `no audit log`
- `default audit log`

Feature operation during downgrade

Downgrading the switch to an earlier release restores the default settings. The IP management address does not change.

E-Tree and Private VLANs

Private VLANs consist of a primary and a secondary VLAN that provide isolation between ports within a Layer 2 service. The E-Tree feature allows private VLANs to traverse an SPBM network by associating a private VLAN with an I-SID.

- For more information about E-Tree, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4800 Series, NN47205-507*.
- For more information about Private VLANs, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series, NN47205-501*.

Fabric Attach enhancements

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

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

The FA feature provides the following enhancements:

- Dynamic Trusted QoS interface updates
- Multiple authentication key support
- Tagging mode on FA Client port updated based on client specific state
- Authentication status data related to the FA and I-SID/VLAN Assignment TLV displayed in the output of the show fa elements command
- Zero Touch Client installation
- FA statistics

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4800 Series, NN47205-507*.

ACLI commands

This feature introduces the following ACLI commands:

- `fa message-authentication key-mode strict`
- `fa message-authentication key-mode standard`
- `fa zero-touch-client`
- `no fa zero-touch-client`
- `default fa zero-touch-client`
- `show fa zero-touch-client`
- `clear fa statistics`
- `show fa statistics`

For more information, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 4800 Series, NN47205-105*.

MLD Proxy

Multicast Listener Discovery (MLD) is the IPv6 equivalent to Internet Group Management Protocol (IGMP) in IPv4, where MLD Proxy provides a function similar to IGMP Proxy.

With MLD snooping enabled, the switch can receive multiple reports for the same multicast group. By using the MLD proxy feature, the switch can consolidate these multiple reports rather than forward each report upstream.

For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series, NN47205-506*.

ACLI commands

This feature introduces the following ACLI commands:

- `ipv6 mld proxy`

- [default] [no] ipv6 mld proxy
- show ipv6 mld-proxy-cache [vlan <1-4094> [group <ipv6>]]

Support standards

The following standards are supported:

- RFC2710 – MLD for IPv6
- RFC3810 – RFC 3810 MLDv2 for IPv6
- RFC4541 – Considerations for IGMP and MLD snooping switches

Password complexity and password aging and lockout policy

Password complexity

The administrator can enforce complexity of the passwords. This feature is enabled automatically after the software upgrade.

An administrator can set complexity rules for the following:

- minimum password length
- required character types used in a password
- number of unique passwords retained in history
- check for sequential or repeated characters within passwords

For more information see, *Configuring Security on Avaya Ethernet Routing Switch 4800 Series, NN47205-505*.

Password aging and lockout policy

Password aging is the number of days that a password is allowed to remain active prior to a forced change.

Lockout policy is the number of consecutive failed login attempts prior to the account lock out. An administrator can re-enable the locked out account.

An administrator can set rules for the following:

- number of days before password expiration
- number of warning days before password expiration
- number of consecutive failed login attempts before lockout
- automatic unlock timer value for disabled accounts due to inactive timeout
- amount of delay time to add after three consecutive failed login attempts within one minute
- ability to force a password change on first login
- number of times a password can be changed in a day
- notification message when a login fail occurs

For more information see, *Configuring Security on Avaya Ethernet Routing Switch 4800 Series, NN47205-505*.

Changed CLI commands

The following CLI commands are changed:

- `password`
- `default password`
- `show password`
- `username lockout-retries <0-100>`
- `username inactive-period <0-360>`

For more information about CLI commands, see *CLI Commands Reference for Avaya Ethernet Routing Switch 4800 Series, NN47205-105*.

Feature operation during upgrade

Passwords are retained when the software is upgraded from a release that does not support Password complexity and Password aging and lockout features.

SHA-2 support for SSH and SSL certificates

Support for SHA-1 is deprecated and SHA-2 is now supported for SSH and SSL certificate. The reason is Microsoft Security Advisory 2880823. According to the announcement, on January 1, 2016, trusting Code Signing Certificates generated with a SHA-1 hashing algorithm will be stopped, and on January 1, 2017, trusting SHA-1 generated SSL certificates will be stopped.

PoE high inrush mode

You can configure a port to power up a non-standard Powered Device (PD) using the `poe poe-power-up-mode` command. The port mode can be configured as high inrush to power up a non-standard PD instantaneously as soon as it is connected.

Configuring PoE power up mode

About this task

To allow non-standard Powered Devices (PD) to draw power from PoE switches by configuring the port power up mode.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure the PoE power up mode:

```
poe poe-power-up-mode [802.3af | high-inrush | port <portlist>]
```


Variable definitions

Use the data in the following table to use the `poe poe-power-up-mode` command.

Variable	Definition
802.3af	Sets the power up mode to normal.
high-inrush	Sets power up mode to high inrush.
port <LINE>	Specify an individual port or list of ports.

RSPAN over MLT/LACP

RSPAN over MLT/LACP enhances the RSPAN feature by allowing the monitor port to be part of a trunk.

For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series, NN47205-502*.

SFP DDI information

The Digital Diagnostic Interface (DDI) feature collects data and monitors alarms and warnings on all the supported SFP, SFP+, and GBIC transceivers. The following lists the information that DDI collects:

- SFP vendor information (including type, wavelength, vendor name, vendor revision/serial, hardware options, CLEI code, and Product Code)
- DDI support information
- DDI alarm and warning threshold values
- temperature
- supply voltage
- transmit bias current
- TX/RX optical power
- transmit power
- receive power measurement
- transceiver calibration

This functionality is supported from the moment the switch finishes its initialization.

For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series, NN47205-502*.

ACLI commands

The following ACLI commands are supported:

- `ddi-logging enable`
- `no ddi-logging`
- `default ddi-logging`
- `show ddi-logging`
- `show interfaces gbic-info`

SPBM IPv4 Shortcuts

In contrast to IP routing or Multiprotocol Label Switching (MPLS), the SPBM IPv4 Shortcuts feature provides a simpler method of forwarding IP packets in an Ethernet network using the preestablished Ethernet forwarding information bases on the Backbone Edge Bridges.

SPBM IPv4 Shortcuts supports the following functionality:

- IP unicast traffic
- IP multicast traffic
- Connectivity Fault Management (CFM) integration
- Equal Cost Multi Paths

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4800 Series*, NN47205-507.

Supported ACLI commands

- `ip-source-address <ip-address>`
- `[no] [default] ip-source-address`
- `spbm <spbm-instance> ip enable`
- `[default] [no] spbm <spbm-instance> ip enable`
- `redistribute direct`
- `redistribute static`
- `[default] [no] redistribute direct enable`
- `[default] [no] redistribute static enable`
- `ip isis apply redistribute direct`
- `ip isis apply redistribute static`
- `ip isis apply redistribute`
- `ip isis maximum-path <1-4>`

For more information about ACLI commands, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 4800 Series*, NN47205-105.

Changed CLI commands

- 12 `ping <ip-address>`
- 12 `traceroute <ip-address>`

Other changes

In the upgrades section, a note was added to show that Release 5.10 operates with 5.8.0.01 diagnostic image or with 5.8.0.03 diagnostic image.

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 4800 Series Software Release 5.10. 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 in ERS 4800 series
Egress queues	Configurable 1–8
MAC addresses	16384
Stacking bandwidth (full stack of 8 units)	Up to 384 Gbps
QoS precedence	16 per ASIC
QoS rules per ASIC	ERS 4826 – 256 rules per precedence in single/128 in double ERS 4850 – 512 rules per precedence in single/256 in double
Maximum number of units in a stack	8
Maximum number of Port Mirroring Instances	4
Maximum Admin Accounts	10 (two default non-deletable users, one with Read-Write (RW) privileges and one with Read-Only (RO) privileges; others can be configured with either RW or RO privileges)
Layer 2	
Concurrent VLANs	1024
Supported VLAN IDs	1 - 4094 (0 and 4095 reserved; 4001 reserved by STP; 4002-4008 reserved by multiple STP groups)
Protocol VLAN types	7

Table continues...

Feature	Maximum Number Supported in ERS 4800 series
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
Spanning Tree Group instances (802.1s)	8
Avaya Spanning Tree Groups	8
DHCP Snooping table entries	1024
Layer 3	
IP Interfaces (VLANs or Router ports)	256
ARP Entries total (local, static & dynamic)	1792
ARP Entries — local (IP interfaces per switch/stack)	256
ARP Entries — static	256
ARP Entries — dynamic	1280
IPv4 Routes total (local, static & dynamic)	2048
IPv4 Static Routes	512 (configurable 0-512)
IPv4 Local Routes	256 (configurable 2-256)
IPv4 Dynamic Routes (RIP & OSPF)	1280 (configurable up to 2046)
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)	10000
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
Fabric Connect (SPB)	
SPB operational mode	Standalone or stack of up to 8 units
SPB nodes per region	450
SPB (IS-IS) adjacencies per node	4
SPB Customer VLANs (C-VLANs) per node	500

Table continues...

Feature	Maximum Number Supported in ERS 4800 series
SPB I-SIDs per node	500
SPB Switched UNIs	500
Number of B-VLANs	2
Number of IS-IS interfaces per node	4
Maximum multicast streams per stack	512
Maximum Layer 2 VSNs with SPBM Multicast per stack	256
Max ETREE/PVLAN per switch/stack	200
Maximum number of different multicast streams supported (identified by source/group IP and ingress C-VLAN)	<p>250</p> <p>The following formula applies:</p> $512 \text{ ENTRIES} \geq L2_VSN + 2 \times MC_STREAMS + 8 \text{ (reserved)}$ <p>Where,</p> <ul style="list-style-type: none"> ENTRIES is the total number of entries supported. L2_VSN is the number of L2_VSNs (with or without IGMP snooping). MC_STREAMS is the number of IP Multicast streams, local + remote. For remote streams, two entries are occupied and for local streams, only one entry is occupied. <p>* Note:</p> <p>For each L2VSN (C-VLAN or Switched-UNI) created on the SPBM device, an entry is occupied in a hardware table. For each multicast stream, two entries are occupied in the same table, one for the source and one for the receiver, on both the source and client BEBs. The total number of entries is 512, where eight entries are unavailable (used internally by the system). The multicast traffic will work only for the streams that occupied the necessary entries in the hardware table. For example, if there are 250 multicast streams in one C-VLAN, 501 hardware entries will be occupied: 250 for the source of the traffic, 250 for the receivers, and one for the C-VLAN.</p>
Miscellaneous	
IGMP v1/v2 multicast groups	512
IGMP v3 multicast groups	512
IGMP Enabled VLANs	256

Table continues...

Feature	Maximum Number Supported in ERS 4800 series
802.1x (EAP) clients per port, running in MHMA	32
802.1x (NEAP) clients per switch/stack	384
802.1x (EAP & NEAP) clients per switch/stack	768
Maximum RADIUS Servers	2
Maximum 802.1X EAP Servers	2
Maximum 802.1X NEAP Servers	2
Maximum RADIUS/EAP/NEAP Servers	6
IPFIX number of sampled flows	100000
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	2
Port Mirroring Instances	4
Port Mirroring: RSPAN destinations	4 per switch or stack
Port Mirroring: RSPAN VLANs	4
Maximum PIM-SM interfaces	16 PIM interfaces (4 active, 12 passive)

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
SPBM		0	0	0	3	0
DHCP		0	0	0	9	1
CFM	Precedence 2	0	0	0	2	2

Table continues...

Feature	Observation	QoS			NonQoS	
	Precedence 1	0	0	0	2	2
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
QoS	Untrusted					
	Precedence 2	1	0	1	0	0
	Precedence 1	1	0	1	0	0
QoS	Unrestricted	0	0	0	0	0
UDP Forwarding		0	0	0	1	1
OSPF		0	0	0	3	0
RIP		0	0	0	1	0
IPFIX		0	0	0	1	1
SLPP Guard		0	0	0	1	1

File names for this release

File names for release 5.10

The following table describes the Avaya Ethernet Routing Switch 4800 Series, Software Release 5.10 software files.

Table 3: Software Release 5.10 components

Module or File Type	Description	File Name	File Size (bytes)
Runtime Software Image	Image for the Avaya Ethernet Routing Switch 4800 Series	4800_5100207s.img	12,945,136

Table continues...

Module or File Type	Description	File Name	File Size (bytes)
Diagnostic Software Image	4800 diagnostic image	4000_58003_diag.bin	1,934,909
		4000_58001_diag.bin	1,934,853
Enterprise Device Manager Help Files	Help files required for Avaya Ethernet Routing Switch 4800 series	ers4000v5100_HELP_EDM.zip	3,614,989
Enterprise Device Manager Plug-in	Avaya Ethernet Routing Switch 4800 series Enterprise Device Manager plug-in for Configuration and Orchestration Manager	ers4000v5.10.0.0.zip	5,099,456
Software Release 5.10 Management Information Base (MIB) Definition Files	MIB definition files	Ethernet_Routing_Switch_4800_MIBs_5.10.0.zip	1,542,102

Supported traps and notifications

For information about SNMP traps generated by the Avaya Ethernet Routing Switch 4000 Series, see *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.

Tested browsers

EDM has been tested with the following web browsers:

- Microsoft Internet Explorer 11.0
- Mozilla Firefox 45.0.2

Software upgrade

To upgrade to the new software release 5.10 on ERS 4800, first verify or upgrade to software image 5.6.5 or 5.7.0, diagnostic image 5.8.0.01 or diagnostic image 5.8.0.03.

After the software and diagnostics image are verified or updated, you can then upgrade the agent version to release 5.10.

*** Note:**

Release 5.10 operates with diagnostic image 5.8.0.01 or with diagnostic image 5.8.0.03.

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

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
5.6.0.15 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
5.6.1.18 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
5.6.2.01 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.2
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
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
5.6.2.01 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
5.6.2.01 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.4
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 5.6.4
5.6.2.01 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.5

Table continues...

Image	Location
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 5.6.5
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
5.8.0.01 Diagnostic Image for the ERS 4800 series.	Diagnostic image released in 5.8
5.8.0.03 Diagnostic Image for the ERS 4800 series.	Diagnostic image released in 5.10

Upgrading the software

Check the image software version for upgrading to release 5.10.

Note:

Release 5.10 operates with diagnostic image 5.8.0.01 or with diagnostic image 5.8.0.03.

Important:

It is necessary to download the diagnostic image to the switch before downloading and running 5.10.

When upgrading from 5.6.0, 5.6.1, 5.6.2, 5.6.3 and 5.6.4 to 5.9.0, upgrade to 5.6.5 or to 5.7 and then proceed with the download of 5.8.0.01 or 5.8.0.03 diagnostic image and 5.10 software image.

Before upgrading, capture the system information using the procedure [Capturing the system information](#) on page 27 and then, upgrade to release 5.10 using any one of the following procedures:

- [Upgrading from 5.6.0, 5.6.1, 5.6.2, 5.6.3 or 5.6.4 to 5.7 and then 5.10](#) on page 28
- [Upgrading from 5.6.5, 5.7, 5.8, 5.9 to 5.10](#) on page 29

If the DHCP snooping or Non-EAP Phone Authentication uses DHCP signature or DHCP relay in the network, see [Upgrade strategy if DHCP snooping DHCP relay or NonEap Phone Authentication use DHCP signature](#) on page 29

Capturing the system information

About this task

Capture and save the system information for future reporting and troubleshooting.

Procedure

1. Enter Global Configuration mode:

Important notices

- ```
enable
configure terminal
```
2. Display the FLASH information.  

```
show flash
```
  3. Display the consolidated system information.  

```
show system verbose
```
  4. Save the ASCII and binary configuration.  

```
copy running-config tftp address [A.B.C.D | WORD] filename [WORD]
copy config tftp address [A.B.C.D | WORD] filename [WORD]
```

## Upgrading from 5.6.0, 5.6.1, 5.6.2, 5.6.3 or 5.6.4 to 5.7 and then 5.10

### About this task

Use the following procedure to upgrade the software image from Release from 5.6.0, 5.6.1, 5.6.2, 5.6.3 or 5.6.4 to 5.7 and then to release 5.10 using ACLI.

#### Note:

Release 5.10 operates with diagnostic image 5.8.0.01 or with diagnostic image 5.8.0.03.

### Procedure

1. Download 5.8.0.01 or 5.8.0.03 diagnostic image from CLI with no-reset.  

```
download address [A.B.C.D | WORD] diag 4000_58001_diag.bin no-reset
```

OR

```
download address [A.B.C.D | WORD] diag 4000_58003_diag.bin no-reset
```
2. Download 5.7.0 software image from CLI with no-reset.  

```
download address [A.B.C.D | WORD] image 4000_570009s.img no-reset
```
3. Display the boot information.  

```
show boot
```
4. Reboot to run software image v5.7.0 and diagnostic image 5.8.0.01 or 5.8.0.03.  

```
boot
```

The unit reboots and runs software image v5.7.0 and diagnostic image 5.8.0.01 or 5.8.0.03.
5. Download 5.10 software image from CLI.  

```
download address [A.B.C.D | WORD] image 4800_5100011s.img
```
6. Save the ASCII and binary configuration on the 5.10 build.  

```
copy running-config tftp address [A.B.C.D | WORD] filename [WORD]
copy config tftp address [A.B.C.D | WORD] filename [WORD]
```

## Upgrading from 5.6.5, 5.7, 5.8, 5.9 to 5.10

### About this task

Use the following procedure to upgrade 5.6.5, 5.7, 5.8, 5.9 to 5.10 using ACLI.

#### \* Note:

Release 5.10 operates with diagnostic image 5.8.0.01 or with diagnostic image 5.8.0.03.

### Procedure

1. Download 5.8.0.1 diagnostic image from CLI with no-reset.

```
download address [A.B.C.D | WORD] diag 4000_58001_diag.bin no-reset
```

OR

```
download address [A.B.C.D | WORD] diag 4000_58003_diag.bin no-reset
```

2. Download 5.10 software image from CLI with no-reset.

```
download address [A.B.C.D | WORD] image 4800_5100011s.img
```

3. Display the boot information.

```
show boot
```

4. Reboot to run software image v5.10.0 and diagnostic image 5.8.0.01 or 5.8.0.03.

```
boot
```

The unit reboots and runs software image v5.10.0 and diagnostic image 5.8.0.01 or 5.8.0.03.

5. Save the ASCII and binary configuration on the 5.10 build.

```
copy running-config tftp address [A.B.C.D | WORD] filename [WORD]
```

```
copy config tftp address [A.B.C.D | WORD] filename [WORD]
```

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

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

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrade strategy | <p>Upgrade all switches in your network if the switches are running software versions prior to the versions mentioned in the following:</p> <ul style="list-style-type: none"> <li>• ERS 25xx: 4.4.3.</li> </ul> <p><b>* Note:</b></p> <p>Note: ERS 25xx is in End of Sales and currently there is no schedule planned for 4.4.3 software version.</p> <ul style="list-style-type: none"> <li>• ERS 35xx: 5.1.2, 5.2.x</li> </ul> |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

*Table continues...*

Important notices

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                       | <ul style="list-style-type: none"> <li>• ERS 4xxx: 5.6.4, 5.7.1, 5.8, 5.9, 5.10</li> <li>• ERS 5xxx: 6.2.8, 6.3.3, 6.6.x, 7.0</li> <li>• VSP 7xxx: 10.3.2, 10.3.3</li> </ul> <p><b>* Note:</b></p> <p>Upgrade the affected ERS switches closest to the client devices first and then progress towards the core.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Issue                                                 | <p>In some previous software releases of the Stackable ERS platforms (ERS 2500, 3500, 4000 and 5000 Series) as well as the VSP 7000, a software issue was found to cause malformed DHCP packets as they were forwarded out of the switch.</p> <p>In the software releases listed in the preceding row, a code change has been made to stop the malformed packets from being generated and also to discard these malformed packets if the switch is receiving them.</p> <p>Due to the nature of the code change, there are potential interaction scenarios between ERS switches running different code versions which will need to be managed within the context of a network upgrade to releases containing the code changes.</p>                                                           |
| Implications if this upgrade strategy is not followed | <p>DHCP packets which previously transitioned the network without issue may now be lost if using ERS switches which utilize mixed agent versions with and without this fix.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Workaround if this upgrade strategy is not followed   | <ul style="list-style-type: none"> <li>• Disable the DHCP features (DHCP snooping, DHCP relay or DHCP signature authentication) on switches running the older software versions so that the malformed DHCP packets are not generated. Implementation of this option is dependent on the network topology that still allows DHCP packets to reach the DHCP server and may require additional configuration changes.</li> <li>• Disabling DHCP snooping or DHCP relay on switches running the software with the fix will prevent malformed DHCP packets from being dropped if they are received from other switches that are not upgraded. Implementation of this option may also require additional configuration changes to ensure that the DHCP requests reach the DHCP server.</li> </ul> |

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

---

## Updating switch software

You can update the version of software running on the switch through either CLI 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 CLI, ensure that CLI is in Privileged EXEC mode.

See the following sections for details about updating switch software:

- [General software upgrade instructions](#) on page 31
- [Changing switch software in CLI](#) on page 31
- [Changing switch software in EDM](#) on page 33

---

## 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 CLI

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

1. Access CLI 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.<br><br>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 <b>tftp-server</b> 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 <b>sftp-server</b> command. When using SFTP, the username parameter can be utilized. <b>Note:</b> 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.                                                                                                                                                                                                                                                                                 |

*Table continues...*



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

---

## Changing switch software in EDM

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

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

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

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

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

**! Important:**

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

---

## Job aid—File System screen fields

The following table describes the File System screen fields.

**Table 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"> <li>• IPv4</li> <li>• IPv6</li> </ul>                                                                                                                                                                                                        |
| 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 <ul style="list-style-type: none"> <li>• dnldConfig: Download a configuration to the switch.</li> <li>• dnldConfigFromSftp: Download a configuration to switch from the SFTP Server*.</li> </ul> |

*Table continues...*

| Field | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <ul style="list-style-type: none"> <li>• dnldConfigFromUsb: Download a configuration to switch using the front panel USB port.</li> <li>• 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.</li> <li>• 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*.</li> <li>• 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*.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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*.</li> <li>• 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*.</li> <li>• 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.</li> <li>• dnldImgIfNewer: Download a new software image to the switch only if it is newer than the one currently in use.</li> <li>• dnldImgNoReset: Download a new software image to the switch. This option replaces the software image on the</li> </ul> |

*Table continues...*

| Field  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <p>switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset.</p> <ul style="list-style-type: none"> <li>• upldConfig: Upload a configuration to the switch from a designated location.</li> <li>• upldConfigToSftp: Upload binary config to SFTP server*.</li> <li>• upldConfigToUsb: Upload binary config to USB port</li> <li>• upldImgToUsb: Upload image to USB port</li> </ul> |
| 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"> <li>• other: No action occurred since the last boot.</li> <li>• inProgress: The selected operation is in progress.</li> <li>• success: The selected operation succeeded.</li> <li>• fail: The selected operation failed.</li> </ul>                                                            |

\* 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      |

*Table continues...*

| Parameter                         | Description                                                                                                        |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 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: ers4800/4800_580001_diag.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: ers4800/4800_580004.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:

1. 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, SFP, and SFP + transceiver compatibility**

| Supported XFPs, SFPs and SFP+s                        | Description            | Minimum software version | Part Number  |
|-------------------------------------------------------|------------------------|--------------------------|--------------|
| <b>Small Form Factor Pluggable (SFP) transceivers</b> |                        |                          |              |
| 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 |

*Table continues...*

| Supported XFPs, SFPs and SFP+s | Description                                                      | Minimum software version | Part Number  |
|--------------------------------|------------------------------------------------------------------|--------------------------|--------------|
| 1000BASE-LX SFP                | 1310 nm LC connector                                             | 5.0.0                    | AA1419015-E5 |
| 1000BASE-CWDM SFP              | 1470 nm LC connector, up to 40 km                                | 5.0.0                    | AA1419025-E5 |
| 1000BASE-CWDM SFP              | 1490 nm LC connector, up to 40 km                                | 5.0.0                    | AA1419026-E5 |
| 1000BASE-CWDM SFP              | 1510 nm LC connector, up to 40 km                                | 5.0.0                    | AA1419027-E5 |
| 1000BASE-CWDM SFP              | 1530 nm LC connector, up to 40km                                 | 5.0.0                    | AA1419028-E5 |
| 1000BASE-CWDM SFP              | 1550 nm LC connector, up to 40 km                                | 5.0.0                    | AA1419029-E5 |
| 1000BASE-CWDM SFP              | 1570 nm LC connector, up to 40 km                                | 5.0.0                    | AA1419030-E5 |
| 1000BASE-CWDM SFP              | 1590 nm LC connector, up to 40 km                                | 5.0.0                    | AA1419031-E5 |
| 1000BASE-CWDM SFP              | 1610 nm LC connector, up to 40 km                                | 5.0.0                    | AA1419032-E5 |
| 1000BASE-CWDM SFP              | 1470 nm LC connector, up to 70 km                                | 5.0.0                    | AA1419033-E5 |
| 1000BASE-CWDM SFP              | 1490 nm LC connector, up to 70 km                                | 5.0.0                    | AA1419034-E5 |
| 1000BASE-CWDM SFP              | 1510 nm LC connector, up to 70 km                                | 5.0.0                    | AA1419035-E5 |
| 1000BASE-CWDM SFP              | 1530 nm LC connector, up to 70 km                                | 5.0.0                    | AA1419036-E5 |
| 1000BASE-CWDM SFP              | 1550 nm LC connector, up to 70 km                                | 5.0.0                    | AA1419037-E5 |
| 1000BASE-CWDM SFP              | 1570 nm LC connector, up to 70 km                                | 5.0.0                    | AA1419038-E5 |
| 1000BASE-CWDM SFP              | 1590 nm LC connector, up to 70 km                                | 5.0.0                    | AA1419039-E5 |
| 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-E6 |
| 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 |

*Table continues...*

Important notices

| Supported XFPs, SFPs and SFP+s | Description                                                 | Minimum software version | Part Number  |
|--------------------------------|-------------------------------------------------------------|--------------------------|--------------|
| 1000BaseXD DDI SFP             | 1310nm LC connector                                         | 5.4.0                    | AA1419050-E6 |
| 1000BaseXD DDI SFP             | 1550nm LC connector                                         | 5.4.0                    | AA1419051-E6 |
| 1000BaseZX DDI SFP             | 1550nm LC connector                                         | 5.4.0                    | AA1419052-E6 |
| 1000BaseCWDM SFP               | 1470nm LC connector, up to 40km                             | 5.4.0                    | AA1419053-E6 |
| 1000BaseCWDM DDI SFP           | 1490nm LC connector, up to 40km                             | 5.4.0                    | AA1419054-E6 |
| 1000BaseCWDM DDI SFP           | 1510nm LC connector, up to 40km                             | 5.4.0                    | AA1419055-E6 |
| 1000BaseCWDM DDI SFP           | 1530nm LC connector, up to 40km                             | 5.4.0                    | AA1419056-E6 |
| 1000BaseCWDM DDI SFP           | 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 |

Table continues...



| Supported XFPs, SFPs and SFP+s               | Description                                                        | Minimum software version | Part Number  |
|----------------------------------------------|--------------------------------------------------------------------|--------------------------|--------------|
| 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 |
| 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 |
| <b>10 Gigabit Ethernet XFP Transceivers</b>  |                                                                    |                          |              |
| 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 |
| <b>10 Gigabit Ethernet SFP+ Transceivers</b> |                                                                    |                          |              |
| 10GBASE-LR SFP+                              | 1-Port 10 Gigabit-LR SFP + (LC) Single mode up to 10 km            | 5.6.0                    | AA1403011-E6 |
| 10GBASE-ER SFP+                              | 1-Port 10 Gigabit-ER SFP + (LC) Single mode up to 40 km            | 5.6.0                    | AA1403013-E6 |
| 10GBASE-SR SFP+                              | 1-Port 10 Gigabit-SR SFP + (LC) Multi-mode fibre up to 300 m       | 5.6.0                    | AA1403015-E6 |
| 10GBASE-LRM SFP+                             | 1-Port 10 Gigabit-LRM SFP+ (LC) Multi-mode fibre up to 220 m       | 5.6.0                    | AA1403017-E6 |
| 10GDAC-10M SFP+                              | SFP+ direct attach cable 10 m                                      | 5.6.0                    | AA1403018-E6 |
| 10GDAC-3M SFP+                               | SFP+ direct attach cable 3 m                                       | 5.6.0                    | AA1403019-E6 |

*Table continues...*

| Supported XFPs, SFPs and SFP+s | Description                   | Minimum software version | Part Number  |
|--------------------------------|-------------------------------|--------------------------|--------------|
| 10GDAC-5M SFP+                 | SFP+ direct attach cable 5 m  | 5.6.0                    | AA1403020-E6 |
| 10GBASE-ZR/ZW SFP+             | 1550 nm 80km SMF              | 5.8.0                    | AA1403016-E6 |
| 10GBASE-ER CWDM SFP+           | 1471 nm Wavelength up to 40km | 5.9                      | AA1403153-E6 |
| 10GBASE-ER CWDM SFP+           | 1491 nm Wavelength up to 40km | 5.9                      | AA1403154-E6 |
| 10GBASE-ER CWDM SFP+           | 1511 nm Wavelength up to 40km | 5.9                      | AA1403155-E6 |
| 10GBASE-ER CWDM SFP+           | 1531 nm Wavelength up to 40km | 5.9                      | AA1403156-E6 |
| 10GBASE-ER CWDM SFP+           | 1551 nm Wavelength up to 40km | 5.9                      | AA1403157-E6 |
| 10GBASE-ER CWDM SFP+           | 1571 nm Wavelength up to 40km | 5.9                      | AA1403158-E6 |
| 10GBASE-ER CWDM SFP+           | 1591 nm Wavelength up to 40km | 5.9                      | AA1403159-E6 |
| 10GBASE-ER CWDM SFP+           | 1611 nm Wavelength up to 40km | 5.9                      | AA1403160-E6 |
| 10GBASE-ER CWDM SFP+           | 1471 nm Wavelength up to 70km | 5.9                      | AA1403161-E6 |
| 10GBASE-ER CWDM SFP+           | 1491 nm Wavelength up to 70km | 5.9                      | AA1403162-E6 |
| 10GBASE-ER CWDM SFP+           | 1510nm Wavelength up to 70km  | 5.9                      | AA1403163-E6 |
| 10GBASE-ER CWDM SFP+           | 1531 nm Wavelength up to 70km | 5.9                      | AA1403164-E6 |
| 10GBASE-ER CWDM SFP+           | 1551 nm Wavelength up to 70km | 5.9                      | AA1403165-E6 |
| 10GBASE-ER CWDM SFP+           | 1571 nm Wavelength up to 70km | 5.9                      | AA1403166-E6 |
| 10GBASE-ER CWDM SFP+           | 1591 nm Wavelength up to 70km | 5.9                      | AA1403167-E6 |
| 10GBASE-ER CWDM SFP+           | 1611 nm Wavelength up to 70km | 5.9                      | AA1403168-E6 |
| 10GBASE-BX10 SFP+              | 10 km                         | 5.10                     | AA1403169-E6 |
| 10GBASE-BX10 SFP+              | 10 km                         | 5.10                     | AA1403170-E6 |

For more information, see *Installing Avaya Ethernet Routing Switch 4800 Series*, NN47205-300 and *Installing Transceivers and Optical Components on Avaya Ethernet Routing Switch 4800 Series*, NN47205-301.

---

## Supported standards, RFCs and MIBs

The following sections list the standards, RFCs and MIBs.

---

### Standards

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

- IEEE 802.1 (Port VLAN, Port & Protocol VLANs, VLAN Name, Protocol Entity)
- IEEE 802.1AB (Link Layer Discovery Protocol)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Trees)
- IEEE 802.1v (VLAN Classification by Protocol and Port)
- IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)
- IEEE 802.1X (EAPOL)
- 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

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

- RFC 768 UDP
- RFC 783 TFTP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet
- RFC 894 IP over Ethernet
- RFC 903 Reverse ARP
- RFC 950 / RFC 791 IP
- RFC 951 BootP
- RFC 958 NTP
- RFC 1058 RIPv1
- RFC 1112 IGMPv1
- RFC 1122 Requirements for Internet hosts
- RFC 1155 SMI
- RFC 1156 MIB for management of TCP/IP
- RFC 1157 SNMP
- RFC 1212 Concise MIB definitions
- RFC 1213 MIB-II
- RFC 1215 SNMP Traps Definition
- RFC 1340 Assigned Numbers
- RFC 1350 TFTP
- RFC 1354 IP Forwarding Table MIB
- RFC 1398 Ethernet MIB
- RFC 1442 SMI for SNMPv2
- RFC 1450 MIB for SNMPv2
- RFC 1493 Bridge MIB
- RFC 1519 Classless Inter-Domain Routing (CIDR)
- RFC 1591 DNS Client

- RFC 1650 Definitions of Managed Objects for Ethernet-like Interfaces
- RFC 1724 / RFC 1389 RIPv2 MIB extensions
- RFC 1769 / RFC 1361 SNMP
- RFC 1886 DNS extensions to support IPv6
- RFC 1908 Coexistence between SNMPv1 & v2
- RFC 1945 HTTP v1.0
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2011 SNMP v2 MIB for IP
- RFC 2012 SNMP v2 MIB for TDP
- RFC 2013 SNMP v2 MIB for UDP
- RFC 2096 IP Forwarding Table MIB
- RFC 2131 / RFC 1541 Dynamic Host Configuration Protocol (DHCP)
- RFC 2138 RADIUS Authentication
- RFC 2139 RADIUS Accounting
- RFC 2236 IGMPv2
- RFC 2328 / RFC 2178 / RFC 1583 OSPFv2
- RFC 2453 RIPv2
- RFC 2454 IPv6 UDP MIB
- RFC 2460 IPv6 Specification
- RFC 2461 IPv6 Neighbor Discovery
- RFC 2464 Transmission of IPv6 packets over Ethernet
- RFC 2474 Differentiated Services (DiffServ)
- RFC 2541 Secure Shell protocol architecture
- RFC 2597 Assured Forwarding PHB Group
- RFC 2598 Expedited Forwarding PHB Group
- RFC 2616 / RFC 2068 HTTP 1.1
- RFC 2660 HTTPS - Secure Web
- RFC 2665 / RFC 1643 Ethernet MIB
- RFC 2674 Q-BRIDGE-MIB
- RFC 2710 Multicast Listener Discovery version 1 (MLDv1)
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2787 Definitions of Managed Objects for VRRP
- RFC 2819 / RFC 1757 / RFC 1271 RMON
- RFC 2851 Textual Conventions for Internet network addresses

## Important notices

- RFC 2863 / RFC 2233 / RFC 1573 Interfaces Group MIB
- RFC 2865 RADIUS
- RFC 2866 / RFC 2138 RADIUS Accounting
- RFC 2869 RADIUS Extensions—Interim updates
- RFC 2933 IGMP MIB
- RFC 3058 RADIUS Authentication
- RFC 3140 / RFC 2836 Per-Hop Behavior Identification codes
- RFC 3162 IPv6 RADIUS Client
- RFC 3246 Expedited Forwarding Per-Hop Behavior
- RFC 3260 / RFC 2475 Architecture for Differentiated Services
- RFC 3289 DiffServ MIBs
- RFC 3410 / RFC 2570 SNMPv3
- RFC 3411 / RFC 2571 SNMP Frameworks
- RFC 3412 / RFC 2572 SNMP Message Processing
- RFC 3413 / RFC 2573 SNMPv3 Applications
- RFC 3414 / RFC 2574 SNMPv3 USM
- RFC 3415 / RFC 2575 SNMPv3 VACM
- RFC 3416 / RFC 1905 SNMP
- RFC 3417 / RFC 1906 SNMP Transport Mappings
- RFC 3418 / RFC 1907 SNMPv2 MIB
- RFC 3513 IPv6 Addressing Architecture
- RFC 3484 Default Address Selection for IPv6
- RFC 3569 Overview of Source Specific Multicast (SSM)
- RFC 3576 Dynamic Authorization Extensions to RADIUS
- RFC 3579 RADIUS support for EAP
- RFC 3584 / RFC 2576 Co-existence of SNMP v1/v2/v3
- RFC 3587 IPv6 Global Unicast Format
- RFC 3596 DNS extensions to support IPv6
- RFC 3621 Power over Ethernet MIB
- RFC 3635 Definitions of Managed Objects for the Ethernet-like Interface Types
- RFC 3768 / RFC 2338 VRRP
- RFC 3810 Multicast Listener Discovery version 2 (MLDv2)
- RFC 3826 AES for the SNMP User-based Security Model
- RFC 3917 Requirements for IPFIX

- RFC 3954 Netflow Services Export v9
- RFC 3993 DHCP Subscriber-ID sub-option
- RFC 4007 Scoped Address Architecture
- RFC 4022 / RFC 2452 TCP MIB
- RFC 4113 UDP MIB
- RFC 4133 / RFC 2737 / RFC 2037 Entity MIB
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Transition Mechanisms for IPv6 Hosts & Routers
- RFC 4250 SSH Protocol Assigned Numbers
- RFC 4251 SSH Protocol Architecture
- RFC 4252 SSH Authentication Protocol
- RFC 4253 SSH Transport Layer Protocol
- RFC 4254 SSH Connection Protocol
- RFC 4291 IPv6 Addressing Architecture
- RFC 4292 IP Forwarding Table MIB
- RFC 4293 IPv6 MIB
- RFC 4344 SSH Transport layer Encryption Modes
- RFC 4345 Improved Arcfour Modes for SSH
- RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6
- RFC 4432 SSHv2 RSA
- RFC 4443 / RFC 2463 ICMPv6 for IPv6
- RFC 4541 Considerations for IGMP and MLD snooping switches
- RFC 4601 Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification
- RFC 4604 / RFC 3376 IGMPv3
- RFC 4673 RADIUS Dynamic Authorization Server MIB
- RFC 4675 RADIUS Attributes for VLAN and Priority Support
- RFC 4716 SSH Public Key File Format
- RFC 4750 / RFC 1850 / RFC 1253 OSPF v2 MIB
- RFC 4789 SNMP over IEEE 802 Networks
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 / RFC 2462 IPv6 Stateless Address Auto-Configuration
- RFC 5010 / RFC 3046 DHCP Relay Agent Information Option 82
- RFC 5101 Specification of the IP Flow Information Export (IPFIX) Protocol for Exchange of IP Traffic
- RFC 5176 / RFC 3576 Dynamic Authorization Extensions to RADIUS

- RFC 5186 IGMPv3/MLDv2 and Multicast Routing Interaction
- RFC 5905 / RFC 4330 / RFC 1305 NTPv4
- RFC 6329 IS-IS Extensions Supporting Shortest Path Bridging

## IPv6 specific RFCs

The following lists supported IPv6 specific RFCs:

- RFC 1981 Path MTU Discovery for IPv6
- 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 2710 Multicast Listener Discovery version 1 (MLDv1)
- RFC 3162 RADIUS and IPv6
- RFC 3484 Default Address Selection for IPv6
- RFC 3810 Multicast Listener Discovery version 2 (MLDv2)
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4291 IPv6 Addressing Architecture
- RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6
- RFC 4443 ICMPv6 for IPv6
- RFC 4541 IGMP and MLD snooping
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Auto-Configuration
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

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 |

*Table continues...*



| Standard | Description                                      | Compliance                                                                                                                                          |
|----------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 in Release 5.10

| Reference number | Description                                                                                                                                                                                                                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERS454800–806    | MHSA: CPU stuck in 100% for almost 50 seconds after clearing CAM (EAP client authenticated)                                                                                                                                                                                                                                                               |
| ERS454800–1053   | FA with EAP: Multiple Standard VLANs/VSA BINDs with ISID=0 are not supported in MHSA in the SBP topology.<br>WORKAROUND: Standard VLAN must be changed to (VLAN:ISID) binding.                                                                                                                                                                            |
| ERS454800–1294   | RFC 3576: Inconsistency between Release 5.9 and 5.9.2 when sending a CoA or Disconnect message for an EAP client with NAS-IP_Address and NAS-Port attributes.<br>All RFC 3576 requests should select a RADIUS authenticated client. Requests using only the port number as the client selection attribute have no impact on port or client configuration. |
| ERS454800–1312   | EAP:FA: When using an FA Server/SPBM mode and MHSA authentication type, the DUT will reject a VSA Vlan/Isid with Isid=0 send by the Radius Server (Vlan:Isid with Isid equal to 0 not supported in FA SPB networks).                                                                                                                                      |
| ERS454800–1326   | EAP: Log message should be generated when a RAV cannot be created                                                                                                                                                                                                                                                                                         |
| ERS454800–2127   | ERS 4000: Auto-negotiation setting change to custom after upgrade.<br>This was closed with No Fix Planned - Working as designed. This limitation is documented in ERS454800–2232.                                                                                                                                                                         |

# Chapter 5: Known issues and limitations

Use the information in this section to learn more about known issues and limitations from Release 5.10. Where appropriate, use workarounds provided for the known issues and limitations.

## Known issues and limitations for Release 5.10

The following table lists known issues and limitations for software Release 5.10.

| Reference number | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERS454800-802    | EDM: SNMP Engine ID cannot be set for users in EDM (inconsistency with CLI)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ERS454800-852    | FA w/ EAP:EAP/NEAP clients are erased during stack to standalone transition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ERS454800-885    | AUTO: lacp can be enabled on ports that have different ipsig settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ERS454800-899    | EDM: i-sid/vlan bindings cannot be created from edm with spbm disabled (inconsistency with cli)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ERS454800-1141   | EDM: Counters for CoA and Disconnect request are not updated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| ERS454800-1312   | EAP: FA: In MHSA mode, an FA Server functioning in SPBM mode rejects VSAs from the RADIUS server that contain VLAN/I-SID bindings with an I-SID value of 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ERS454800-1315   | SSH: It may take close to five minutes to generate an SSH key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ERS454800-1435   | <p>The BU's CPU goes to 100% and the console will freeze when flooding with TCP SYN packets send to port 23. This only happens with a defaulted DUT.</p> <p><b>Workaround:</b> Use the following QoS settings to filter all SYN traffic sent to the management IP that is not originating from a known IP address.</p> <pre> qos traffic-profile classifier name attack addr-type ipv4 src-ip 10.114.139.0/24 dst-ip 10.114.139.10/32 protocol 6 tcp-control s block requirement eval-order 1 committed-rate 64 committed-burst- size 4 drop-out-action enable qos traffic-profile classifier name attack addr-type ipv4 src-ip 10.100.94.0/24 dst-ip 10.10.114.139.10/32 protocol 6 tcp-control s block requirement eval-order 2 committed-rate 64 committed-burst- size 4 drop-out-action enable qos traffic-profile classifier name attack addr-type ipv4 dst-ip 10.114.139.10/32 protocol 6 tcp-control s drop-action enable block requirement eval-order 100 drop-out-action enable qos traffic-profile classifier name attack addr-type ipv4 protocol 6 tcp-control s block requirement eval-order 101 committed-rate 1024 committed-burst-size 4 drop-out-action enable </pre> |

*Table continues...*



| Reference number | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <pre>qos traffic-profile set port 1/25 name attack meter-mode classifier track-statistics individual</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ERS454800-1618   | EDM: Add support for newer Internet Explorer versions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ERS454800-1937   | <p>EAP+FA Proxy Standalone: Console freeze for about 3 minutes when issuing the command "clear eapol non-eap"</p> <p><b>Workaround:</b> In setups with hundreds of NEAP clients, trying to remove all of them using <code>clear eapol non-eap</code> may take a few minutes. Console will be available only after the removal is finished.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ERS454800-2168   | FA proxy standalone w/ EAP scaling: BU clients are in radius timeout state after bouncing all interfaces simultaneously                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ERS454800-2170   | <p>EAP, MHSA, scaling: it takes 2-3 minutes for console to recover after issuing „clear eap non-eap” command</p> <p><b>Workaround:</b> In setups with hundreds of NEAP clients, trying to remove all of them using <code>clear eapol non-eap</code> may take a few minutes. Console will be available only after the removal is finished.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ERS454800-2184   | EAP, MHSA, GV, FOV, scaling: slow console response and high cpu rate when clients are transitioning from guest unauthenticated to fail open                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ERS454800-2357   | EDM: An isolated port is not added into vlan, if there is already an isolated port, when using EDM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ERS454800-2365   | <p>IPSC Unicast: Multiple DHCP-Relays aren't working in IPSC setup</p> <p> <b>Note:</b></p> <p>The issue appears in a setup with IPSCU and dhcp-relay rules configured on BEBs. The particularity of the case is that dhcp packets need to be successively relayed on two BEBs in order to reach the dhcp server network. Reachability between BEB's attached networks is achieved through ISIS routing (static and directly connected routes redistribution). The dhcp discover packets received from a client directly attached to a BEB are relayed and transmitted to another BEB according to the routing table. On the receiving end, the second BEB is not able to further relay the discover packets because no forwarding path can be configured to serve the packets received on the NNI interface. Thus, the packets are being dropped.</p> |
| ERS454800-2421   | <p>Auto: EAP: EAP users lost after RADIUS server is unreachable - FOV continuity mode enabled</p> <p><b>Workaround:</b> In setups with a big number of EAP/NEAP clients, moving to FOV may result in losing of some clients.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| ERS454800-2424   | <p>SPBM: L2VSN traffic ingressing MLT is doubled or filtered (depending on SMAC and DMAC)</p> <p><b>Workaround:</b> UNI MLTs are not supported with SPB.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ERS454800-2428   | EDM: Error ('No creation, the OID index is not correct') when trying to insert L2 TraceMRoute in EDM (it works with same parameters in CLI)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table continues...

| Reference number | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERS454800–2429   | EAP, MHSA: clients are tracked with radius status set to <code>pending radius authentication</code> when radius server is not configured                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ERS454800–2431   | ECMP:MLT: ECMP static routes become inactive after creating a MLT using the ports connected to the NH (specific scenario)<br><br><b>Workaround:</b> Enable L2 operation (create MLT) before L3 operation (enable IP Routing).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ERS454800–2442   | IP Shortcuts Multicast: Console may lock and messages displayed ( <code>ifconfig: ipcom_socket() failed: Too many open files</code> ) after disable/enable ip routing 5-10 times in system setup with large config and traffic running                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ERS454800–2453   | IP Shortcuts Multicasts: <code>show ip igmp sender</code> displays entries for vlan 4060, port sender: spb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ERS454800–2462   | <code>show ip igmp sender</code> displays group only on one of the ports on which stream is received (streams with same group dest received on multiple ports)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ERS454800–2463   | EDM: Incorrect port number displayed for multicast streams (Configuration -> IP -> IGMP -> Sender)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ERS454800–2464   | Poe High-Inrush Mode: Inconsistency between CLI and EDM regarding Power Up Mode configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ERS454800–2469   | EAP, MHSA: clients are tracked with radius status set to “pending radius authentication” when radius server is not configured                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ERS454800–2473   | AGS: NTP is unable to sync when using key type MD5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ERS454800–2493   | AUR is not performed on BU on 2 unit stack if stack is in SPBM mode.<br><br> <b>Note:</b><br>As a result of this issue, the enhancement is limited in the flowing way: if on a stack of two units there are settings that originally required a reboot to configure (like SPBM enabled, SPBM reserved-port enabled, different STP mode or different QoS queue settings), replacing a Base Unit will not work directly. If the replacement Base Unit is defaulted, when connecting it to the non-base unit that was part of the stack, the non-base will try to match the settings of the base and will reboot itself. This means that the backup configuration will be lost and the replacement base unit will NOT get the configuration of the old base unit. As a workaround for this, the replacement unit should be configured to match the settings that require a reboot before connecting it to the stack. For example if the stack originally had SPBM enabled, before adding the replacement unit to the stack, spbm should be enabled on it. |
| ERS454800–2496   | Counter of CLI command <code>show isis spbm i-sid all/config/discover</code> is incorrect (showing 0 for discovered i-sids and incorrect value for configured i-sids)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## IPv6 limitations

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

**Table 10: IPv6 limitations**

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

# Chapter 6: Resources

---

## Support

Go to 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.

---

## Documentation

For a list of the documentation for this product and more information about documents on how to configure other switch features, see *Documentation Reference for Avaya Ethernet Routing Switch 4800 Series*, NN47205–101.

For more information on new features of the switch and important information about the latest release, see *Release Notes for Avaya Ethernet Routing Switch 4800 Series*, NN47205-400.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.

For the current documentation, see the Avaya Support web site: [www.avaya.com/support](http://www.avaya.com/support).

---

## 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 |

---

## Viewing Avaya Mentor videos

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

### About this task

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

### Procedure

- To find videos on the Avaya Support website, go to <http://support.avaya.com> and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to [www.youtube.com/AvayaMentor](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 website.

 **Note:**

Videos are not available for all products.

---

## Searching a documentation 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`.



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.

---

## Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

### About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

### Procedure

1. In an Internet browser, go to <https://support.avaya.com>.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.

**GENERAL NOTIFICATIONS**  
1/5 Notifications Selected

|                                                 |                                     |
|-------------------------------------------------|-------------------------------------|
| End of Sale and/or Manufacturer Support Notices | <input type="checkbox"/>            |
| Product Correction Notices (PCN)                | <input checked="" type="checkbox"/> |
| Product Support Notices                         | <input type="checkbox"/>            |
| Security Advisories                             | <input type="checkbox"/>            |
| Services Support Notices                        | <input type="checkbox"/>            |

**UPDATE >>**

6. Click **OK**.
7. In the **PRODUCT NOTIFICATIONS** area, click **Add More Products**.

**PRODUCT NOTIFICATIONS** [Add More Products](#)

Show Details **1 Notices**

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.

| PRODUCTS                                    | My Notifications                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual Services Platform 7000              | <b>VIRTUAL SERVICES PLATFORM 7000</b><br>Select a Release Version<br>All and Future<br>Administration and System Programming <input type="checkbox"/><br>Application Developer Information <input type="checkbox"/><br>Application Notes <input type="checkbox"/><br>Application and Technical Notes <input checked="" type="checkbox"/><br>Declarations of Conformity <input type="checkbox"/><br>Documentation Library <input checked="" type="checkbox"/><br><b>SUBMIT &gt;&gt;</b> |
| Virtualization Provisioning Service         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Visual Messenger™ for OCTEL® 250/350        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Visual Vectors                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Visualization Performance and Fault Manager |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Voice Portal                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Voice over IP Monitoring                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| W310 Wireless LAN Gateway                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| WLAN 2200 Series                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| WLAN Handset 2200 Series                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

11. Click **Submit**.