Release Notes for Avaya Ethernet Routing Switch 4800 Series

Release 5.8
NN47205-400
Issue 11.06
August 2016

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 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, 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. 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 Designated Processor that hosts 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 on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, 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 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.

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.

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

Purpose

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Avaya Ethernet Routing Switch 4800 Series, Software Release 5.8.

Note:

Release 5.8 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*, NN47205-400— Software Release 5.8.

Features

See the following sections for information about the new features in ERS 4800 series.

Circuitless IP

You can use a circuitless IP (CLIP) interface to ensure connectivity to an ERS 4800 series device, as long as a network path is available to reach the device. CLIP allows the flexibility of assigning an IP address for various functions without physically binding it to an interface. This is useful for routing protocols such as Open Shortest Path First (OSPF) where the router ID must be the IP address of an interface that is always up and reachable. In Release 5.8, the IP addresses configured for CLIP do not determine the OSPF router ID.

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

Fabric Attach

With the Fabric Attach (FA) feature you can extend the fabric edge to devices that do not have full Shortest Path Bridging MAC (SPBM) support. Fabric Attach automates the connection of non-fabric capable devices to an Avaya Fabric Connect enabled network.

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

IPv6 First Hop Security

IPv6 First Hop Security (FHS) addresses the security concerns associated with Router Discovery, Neighbor Discovery, and Dynamic Host Configuration Protocol version 6 (DHCPv6). First Hop Security contains majority of the RIPE 554 mandatory requirements for Layer 2 switches. This includes the following:

- DHCPv6 guard or DHCPv6 filtering
- RA guard or Router Advertisement filtering
- Dynamic IPv6 Neighbor solicitation or advertisement inspection
- Neighbor reachability detection inspection
- Duplicate Address Detection inspection

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

Lockout for failed logon attempts

This feature is applicable for all the administrative connections (telnet, SSH, and web). If the consecutive attempts to log on to the administrative connections fail, the user account used for connecting is locked out for a configurable amount of time. The default lockout interval is one minute. The number of consecutive logon attempts allowed is also configurable and the default value is three.

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

Multicast Listener Discovery (MLD) snooping

The MLD snooping is an IPv6 multicast constraining mechanism running on Layer 2 devices. When MLD snooping is enabled on a VLAN, the Ethernet Routing Switch examines the MLD messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. Based on the learning, the switch forwards multicast traffic only to those interfaces in the VLAN that are connected to the interested receivers instead of flooding traffic to all the interfaces.

MLD is the direct IPv6 replacement for the Internet Group Management Protocol (IGMP) protocol used in IPv4. There are three versions of IGMP, and two versions of MLD. IGMPv2 is equivalent in function to MLDv1 and IGMPv3 is equivalent to MLDv2.

MLD is compliant with the following requests for comment (RFC):

- RFC 2710 —MLDv1
- RFC 3810 —MLDv2
- RFC 4541 — IGMP and MLD snooping

The following are the limitations:

- IPv6 MLD proxy and send query functions are not supported.
- Multicast Flood Control (MFC) is not supported.
- Static mrouter ports cannot be configured on Link Aggregation Control Protocol (LACP) and Port Mirroring monitors.
- IPv6 supports unknown-mcast-allow-flood and unknown-mcast-no-flood. Maximum entries supported for allow flood (384 entries) – Maximum MAC entries supported (128 entries) + Maximum IPv4 entries (128 entries) + Maximum IPv6 entries (128 entries).

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

Multiple local RW and RO user accounts

This feature allows creating eight more users in addition to default read-only (RO) and read-write (RW) users. Each user can access the switch through the local serial port, telnet, or HTTP (web). User actions are visible through the analysis of audit records.

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

Protocol Independent Multicast-Sparse Mode (PIM-SM)

Protocol Independent Multicast-Sparse Mode (PIM-SM), defined in RFC 4601, supports multicast groups spread out across large areas of a company or the Internet. PIM-SM is one of a number of multicast routing protocols, but unlike dense-mode protocols that flood multicast traffic to all routers over an entire internetwork, PIM-SM directs source traffic to a single point in the network and receivers request to receive the multicast traffic, thus reducing traffic flow over wide area network (WAN) links and minimizing the overhead costs of processing unwanted multicast packets.

With the positioning as the DR-Edge, the following topology recommendations must be considered:

- Not recommended to be used as a candidate RP
- Not recommended to be used as the boot strap router (BSR)
- Not recommended to be used in multi-access LAN
- Not recommended to be used as an Intermediate Router

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

QoS queue statistics

You can use QoS queue statistics for network and configuration diagnostic. Because egress congestion is identified on a per-queue basis with this feature, informed decisions are possible when configuring traffic prioritization and interface or queue shaping.

For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504

Storm Control

This feature provides granular control of broadcast, multicast, and unicast traffic rates on a per-port basis. Broadcast, multicast, and unicast traffic rates can be individually or collectively controlled on a switch or switch stack by setting the following: low-watermark and high-watermark values in packets per second (pps), polling interval value, action type, and SNMP traps. When a high-watermark is exceeded, an action of **none**, **drop**, or **shutdown** can be applied to the traffic type.

A defined action is reversed, or ceases, when the traffic rate in pps falls below the low-watermark setting. When an action of **drop** is used, traffic is dropped when traffic exceeds the high-watermark and does not resume forwarding until the traffic rate falls below the low-watermark. When the action of **shutdown** is used, the switch port is administratively shut down when traffic exceeds the high-watermark and requires administrator intervention to re-enable the switch port to resume traffic forwarding.

The Storm Control feature includes logging of watermark crossings and sending of traps for the low and high watermark crossings. Traps for high watermark exceeded can be sent repeatedly at a user-specified interval.

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

Other feature enhancements

The following are the other feature enhancements in ERS 4800 series:

- Support for 16K MAC address learning.
- QoS filter precedence is increased from 8 to 16.

- FLASH space for agent code is increased from 10 MB to 20 MB.

For more information, see Supported software and hardware capabilities on page 32.

Last change timestamp in ACLI

The **`show interfaces`** command output displays last change timestamp. For more information about the command output display, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.

New hardware support

10GBase-ZR/ZW 80 KM is supported

This SFP+ module enables 10G Ethernet utilization over long distances. This can be used when acquiring dark fiber from a service provider to create an Shortest Path Bridging (SPB) WAN within an enterprise.

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

Overview of features and hardware models by release

This section provides an overview of the Ethernet Routing Switch 4000 series software features and hardware models introduced in Releases 5.0 to 5.7. The features during the Releases 5.0.x to 5.5.x are merged and available in the Release 5.6..

Features for Releases

For more information about features and their configuration, see the documents listed in the respective sections.

The DAUR feature is obsolete as of Release 5.6.

The NSNA feature is obsolete as of Release 5.7.

Features	New in release	
	5.6.x	5.7.x
802.1X-2004 support For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
ADAC Uplink over SPBM For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.		x
802.1X Block subsequent MAC authentication		x

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		
boot partial-default command For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		x
Change RADIUS Password For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
Circuitless IP		
Default all EAP settings For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
EAP and NEAP separation For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
EAP-MD5 authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
eapol multihost mac-max For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
EDM improved download support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		x
EDM inactivity time out For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		x
FastEthernet replaced with Ethernet		x
Show FLASH History For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		x
Jumbo frames		x

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		
Link-state tracking For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		x
List command For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102.		x
MAC security port lockout For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
MLT/DMLT/LAG dynamic VLAN behavior changes For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		x
NEAP IP Phone support enhancement		x
NEAP not member of VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
Password change via EDM For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
RADIUS NEAP password configurable key For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
Remote Switch Port ANalyzer For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.		x
RO user access to telnet and SSH For more information, see*Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		x
Run Scripts For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		x
SFTP License and DHCP external support		x

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		
Show VLAN interface verbose command For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.		x
SLA Monitor For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.		x
SPBM For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4800 Series*, NN47205-507.		x
Default IP For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Run IP Office Script For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Fail Open VLAN Continuity mode For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
User Based Policies For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
SLAMon Agent For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
Ethernet Routing Switch 4500-PWR+ and 4800 Revision 10 Hardware Support	x	
802.3at LLDP based discovery For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
Syslog Support for 802.1X/EAP/NEAP/UBP For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Trace Support for 802.1X For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Black Hole Improvements	x	
show ip netstat For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Disable MAC Learning For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
Equal Cost MultiPath (ECMP) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506	x	
Industry Standard CLI Improvements	x	
Internet Group Management Protocol (IGMP) Querier For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
Internet Group Management Protocol (IGMP) version 3 Snooping and Proxy For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
IP Phone Automatic PoE Changes For more information, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 4800 Series*, NN47205-105.	x	
Layer 3 Brouter Port For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
Many to Many Port Mirroring	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.		
MLT/DMLT/LAG Dynamic VLAN Changes For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Network Time Protocol (NTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Ping Source Address	x	
Secure File Transfer Protocol (SFTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
SFP+ and Additional SFP Support For more information, see *Installing Transceivers and Optical Components on Avaya Ethernet Routing Switch 4800 Series*, NN47205-301.	x	
Show Flash Function For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
SSH Client For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
SSH RSA Authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Stack Health Monitoring and Recovery For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
Static FDB MAC Entry For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
Terminal Mode Permanent Setting	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
Trace Functions For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
VLAN Scaling	x	
Voice VLAN Integration For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
New Avaya Ethernet Routing Switch 4000 Series models	x	
Avaya Identity Engines Ignition Server For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1AB customization For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
802.1X non-EAP Accounting For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1X non-EAP re-authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1AB new default parameters For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
AUR enhancement For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
DHCP snooping external save For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
EAP Fail Open with multi-VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Layer 3 Virtual Router Redundancy Protocol	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.		
RADIUS EAP or non-EAP requests from different servers For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
SLPP Guard For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
SNMP Trap enhancements For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
STP BPDU filtering ignore-self For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
Unified Authentication	x	
VLACP enhancements For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
802.1AB integration For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
802.1AB Avaya PoE Conservation Level Request TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
802.1AB Avaya Call server TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
802.1AB Avaya File server TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
802.1AB Avaya 802.1Q Framing TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
802.1AB Avaya Phone IP TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Ability to set password, username and type of security for any switch in stack For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505	x	
ASCII Generator	x	
Enterprise Device Manager	x	
802.1AB (LLDP) MED Network Policy CLI For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
802.1D Compliancy Support For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
ADAC and Auto QoS Interoperability	x	
ADAC Enhancements	x	
Additional SFP Support For more information, see *Installing Transceivers and Optical Components on Avaya Ethernet Routing Switch 4800 Series*, NN47205-301.	x	
Automatic QoS and 802.1AB MED Interoperability	x	
DHCP Client For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500, *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
DHCP Option 82 Support For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
DHCP Snooping Improvements For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Dual Syslog Server Support For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
Dynamic Route Table Allocation For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
EAP and non-EAP MultiVLAN capability For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Energy Saver For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x	
Erasable ACLI Audit Log For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
IPFIX For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and*Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x	
MLT and LAG Scaling For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Non-Local Static Routes For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
Open Shortest Path First	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.		
QoS Agent Operational Mode For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
QoS DSCP Mutation For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
QoS Egress Queue Shaping For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
QoS IP/L2 Filter Options For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
QoS Queue Set Support For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
RADIUS Accounting Enhancements (RFC2866) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
RADIUS Server Reachability For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Routing Information Protocol For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
Routing Policies For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
Running Configuration ACLI Display Commands For more information, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 4800 Series*, NN47205-105.	x	
Show Software Status	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.		
Software Licensing For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102.	x	
Sticky MAC Address For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Time Delay Reflectometer For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Traffic Profile Filter Set Support For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
Auto Detection Auto Configuration (ADAC) - modify the 802.1AB detection mechanism used in ADAC to work correctly with the Avaya IP handsets	x	
802.1X or Non-EAP and Guest VLAN on same port For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1X or Non-EAP with Fail_Open VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1X or Non-EAP with VLAN name For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1X or Non-EAP Last Assigned VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1X or Non-EAP use with Wake on LAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
RADIUS Management Accounting For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
RADIUS Request use Management IP	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		
SNMP traps for DHCP snooping/DAI/IPSG For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
Disable CLI audit log command For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Configure asset ID For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Show Environmental For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
Automatic QoS For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
MLT enable/disable whole trunk (MLT shutdown ports on disable) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
ASCII Download Enhancements For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
MAC Flush For more information, see*Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
WebUI MIB Web Page	x	
WebUI Trap Web Page	x	
RADIUS Assigned VLAN update for 802.1x - use most recent RADIUS VLAN enhancement	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		
Sticky MAC Address For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
IP local and static routes For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
BOOTP and DHCP RELAY For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
IP Source Guard For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
TACACS+ For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
802.1X RFC3576 For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1AB MED support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
802.1AB location TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
IPv6 management For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
JDM PoE enhancements	x	
Increase PoE power	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.		
Backup CONFIG file For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500, *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x	
IP.CFG enhancements For more information, see *Installing Avaya Ethernet Routing Switch 4800 Series*, NN47205-300 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x	
Stack health check For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
Disable USB and console For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Extended password history For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Stack Forced Mode For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
AUR improvements For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500, *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
Diagnostics AUR (DAUR)	x	
RSTP SNMP traps For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
Extended IP Manager For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
VLACP enhancement For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
CPU utilization For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502	x	
Multi-Link Trunking For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
RSTP traps For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
RADIUS assigned VLAN update for 802.1x —use most recent RADIUS VLAN enhancement For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Nortel Secure Network Access (NSNA)	x	
DHCP snooping For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700, *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
600 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.		
Dynamic ARP inspection For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1x multiple host single authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
802.1x NEAP support (MAC authentication) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
ADAC (including 802.1ab support) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Virtual LACP For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
BPDU filter For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x	
Logout CLI enhancement	x	
Factory default command	x	
Writer memory and save config command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102	x	
Autosave configuration enhancement For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
Username password enhancement For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
ASCII script config support	x	
New unit quick to config For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Improved syslog capabilities For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
Stack counters For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
Stack monitor For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x	
Configurable SNMP trap port For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Stack loopback tests For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
Port operational status enhancements For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
Show Port enhancement For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502 and *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
RMON scaling For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
ASCII configuration file generator For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Using ACLI and EDM on Avaya Ethernet Routing Switch 4800 Series*, NN47205-102.	x	
Automatic Unit Replacement (AUR) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
Autotopology (802.1ab, SONMP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Boot/DHCP address assignment (RFC 1542)	x	
Broadcast rate limiting	x	
Custom Auto-Negotiation Advertisement (CANA) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Distributed MultiLink Trunking (DMLT) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
EAPoL (802.1x) SHSA/MHMA and Guest VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Flow Control on gigabit Ethernet ports (802.3x) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Independent VLAN Learning (IVL) support For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501 .	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
Internet Group Management Protocol version 2 (IGMPv2, RFC 2236) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
Proxy and snooping support For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4800 Series*, NN47205-506.	x	
Java Device Manager (JDM) support	x	
Link Aggregation (802.3ad) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Link Layer Discovery Protocol (802.1AB) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
MultiLink Trunking (MLT) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
Multiple Spanning Tree groups (802.1s) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
CLI	x	
Ping command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Port mirroring (including ingress and egress) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502.	x	
Port-based VLAN support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500 and *Configuring VLANs, Spanning Tree, and Multi-Link Trunking*	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
on Avaya Ethernet Routing Switch 4800 Series, NN47205-501.		
Power over Ethernet (PoE, 802.3af) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Protocol-based VLAN support (including IPv6 protocol VLANs) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
QoS - Diffserv Code Points (DSCP RFC2998) marking and classification For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
Quality of Service (QoS) - 802.1q For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
Quality of Service (QoS) - Layer 2 to Layer 4 filtering and policies For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
Quality of Service (QoS) - Offset filtering (first 80 bytes) For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4800 Series*, NN47205-504.	x	
Quick start command and Web interface	x	
Rapid Spanning Tree Protocol (802.1w) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
Reload command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Remote Authentication Dial-In User Server (RADIUS) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505 and *Troubleshooting Avaya Ethernet Routing Switch 4800 Series*, NN47205-700.	x	
Remote Monitoring (RMON)	x	

Table continues…

Features	New in release	
	5.6.x	5.7.x
For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4800 Series*, NN47205-502		
Resilient stacking	x	
Secure Shell (SSH, SSHv2) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Simple Network Management Protocol (SNMP, SNMPv3) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4800 Series*, NN47205-505.	x	
Simple Network Time Protocol (SNTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Spanning Tree Protocol Group (802.1D, 802.1t) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4800 Series*, NN47205-501.	x	
Telnet server and client For more information, see *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x	
Trivial File Transfer Protocol (TFTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4800 Series*, NN47205-500.	x	
Web User Interface (http and https)	x	

Other changes

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

Document title change

Release Notes for Avaya Ethernet Routing Switch 4000 Series is renamed *Release Notes for Avaya Ethernet Routing Switch 4800 Series*.

Introduction chapter

Information about Related resources and Support are moved to the last chapter in this document.

Overview of features and hardware models by release

This section provides an overview of the software features and hardware models introduced in Releases 5.0 to 5.7.

Supported RFCs

RFCs 4601 and 3810 are added to the existing list.

For more information, see Supported standards, RFCs and MIBs on page 55.

IPv6 specific RFCs

RFCs 4429 and 3484 are added to the existing list.

For more information, see Supported standards, RFCs and MIBs on page 55.

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 5.8. 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	512 rules per precedence
Maximum number of units in a stack	8
Maximum number of Port Mirroring Instances	4
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
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

Table continues…

Feature	Maximum Number Supported in ERS 4800 series
Avaya Spanning Tree Groups	8
DHCP Snooping table entries	1024
Layer 3	
IP Interfaces (VLANs or Brouter ports)	64 (configurable up to 256)
ARP Entries total (local, static & dynamic)	1792
ARP Entries — local (IP interfaces per switch/stack)	64 (configurable up to 256)
ARP Entries — static	256
ARP Entries — dynamic	1280
IPv4 Routes total (local, static & dynamic)	512
IPv4 Static Routes	32 (configurable 0-256)
IPv4 Local Routes	64 (configurable 2-256)
IPv4 Dynamic Routes (RIP & OSPF)	416 (configurable up to 510)
Dynamic Routing Interfaces (RIP & OSPF)	64
OSPF Areas	4 (3 areas plus area 0)
OSPF Adjacencies (devices per OSPF Area)	16
OSPF Link State Advertisements (LSA)	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
VENA 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
SPB I-SIDs per node	500
SPB Switched UNIs	500
Number of B-VLANs	2
Number of IS-IS interfaces per node	4
C-VLANs per switch/stack (per node)	2000
Switched UNIs	4094

Table continues…

Feature	Maximum Number Supported in ERS 4800 series
Transparent UNIs (per node)	255
L2 VSN I-SIDs per switch/stack (per node)	2000
L3 VSN I-SIDs per switch/stack (per node)	24
Multicast I-SIDs (as BEB and/or BCB)	3000
Multicast over L2 VSNs	1000
Multicast over L3 VSNs	24
Multicast over IP Shortcuts	256
IP interfaces with Multicast enabled	256
Unique multicast streams sourced per node	
ECMP Paths	4
IP Routes in Global Router (GRT)	10000 per VRF, 16000 per switch
Backbone-MACs (B-MACs per node)	1000
MAC entries	32000
Nodes per region	500
IS-IS interfaces	24
IS-IS adjacencies per node	24
IS-IS IP Routes	16000
Miscellaneous	
IGMP v1/v2 multicast groups	512
IGMP v3 multicast groups	512
IGMP Enabled VLANs	256
802.1x (EAP) clients per port, running in MHMA	32
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

Table continues…

Feature	Maximum Number Supported in ERS 4800 series
Link State Tracking: Instances	2
Port Mirroring Instances	4
Port Mirroring: RSPAN VLANs	4
Port Mirroring: RSPAN destinations	4 per switch or stack
Maximum Admin accounts	25
Maximum PIM-SM interfaces	16 PIM interfaces (4 active, 12 passive)
Maximum multicast streams	256 per stack

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
	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

Table continues…

Feature	Observation	QoS			NonQos	
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 5.8

The following table describes the Avaya Ethernet Routing Switch 4800 Series, Software Release 5.8 software files. File sizes are approximate.

Table 3: Software Release 5.8 components

Module or File Type	Description	File Name	File Size (bytes)
Standard Runtime Software Image	Standard image for the Avaya Ethernet Routing Switch 4800 Series	4800_580004.img	10,722,420
Secure Runtime Software Image	Secure image for the Avaya Ethernet Routing Switch 4800 Series	4800_580005s.img	10,999,212
Diagnostic Software Image	4800 diagnostic image	4000_58001_diag.bin	1,934,853
Enterprise Device Manager Help Files	Help files required for Avaya Ethernet Routing Switch 4800 series	ers4000v580_HELP_EDM.zip	3,643,644
Enterprise Device Manager Plug-in	Avaya Ethernet Routing Switch 4800 series Enterprise Device Manager plug-in for Configuration and Orchestration Manager	ers4000v5.8.0.0.zip	5,079,950
Software Release 5.8 Management	MIB definition files	Ethernet_Routing_Switch_4800_MIBs_5.8.0.zip	1,563,066

Table continues…

Module or File Type	Description	File Name	File Size (bytes)
Information Base (MIB) Definition Files			
Ethernet Routing Switch 4800 Complete Software Package v5.8	Complete Software Package	4800_5800.tar.gz	33,309,135

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.

Supported Web browsers for Enterprise Device Manager

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

- Microsoft Internet Explorer versions 7.0 and 8.0. For higher versions, you must use Internet Explorer in compatibility mode.
- Mozilla Firefox version 23.0

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

Software upgrade

To upgrade to the new software release 5.9 on ERS 4800, first verify or upgrade to software image 5.6.5 or 5.7.0, diagnostic image 5.8.0.

After the software and diagnostics image are verified or updated, you can then upgrade the agent version to release 5.9.

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

Table continues…

Image	Location
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
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

Table continues…

Image	Location
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
5.9 Diagnostic Image for the ERS 4800 series.	Diagnostic image released in 5.9

Upgrading Avaya Ethernet Routing Switch 4800 series

Check the image software version for upgrading to release 5.8. Before upgrading, capture the system information using the procedure Capturing the system information on page 39 and then, upgrade to release 5.8 using any one of the following procedures:

- Upgrading from 5.6.0, 5.6.1, 5.6.2, 5.6.3, 5.6.4 to 5.7 and then, 5.8 on page 39
- Upgrading from 5.6.5 and 5.7 to 5.8 on page 40

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 41

Capturing the system information

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   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 5.9

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 5.9 using ACLI.

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
   ```

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 5.8.0.1

   ```
   boot
   ```

   The unit reboots and runs software image v5.7.0 and diagnostic image 5.8.0.1

5. Download 5.9.0 software image from CLI.

   ```
   download address [A.B.C.D | WORD] image 4000_590135s.img
   ```

6. Save the ASCII and binary configuration on the 5.9 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 to 5.9

About this task

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

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
   ```

2. Download 5.8 software image from CLI with no-reset.

   ```
   download address [A.B.C.D | WORD] image 4000_590135s.img
   ```

3. Display the boot information.

   ```
   show boot
   ```

4. Reboot to run software image v5.9.0 and diagnostic image 5.8.0.1.

   ```
   boot
   ```

   The unit reboots and runs software image v5.9.0 and diagnostic image 5.8.0.1.

5. Save the ASCII and binary configuration on the 5.9 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	Upgrade all switches in your network if the switches are running software versions prior to the versions mentioned in the following: • ERS 25xx: 4.4.3. **Note:** Note: ERS 25xx is in End of Sales and currently there is no schedule planned for 4.4.3 software version. • ERS 35xx: 5.1.2, 5.2.x • ERS 4xxx: 5.6.4, 5.7.1, 5.8.x • ERS 5xxx: 6.2.8, 6.3.3, 6.6.x • VSP 7xxx: 10.3.2, 10.4.x **Note:** Upgrade the affected ERS switches closest to the client devices first and then progress towards the core.
Issue	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. 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. 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.
Implications if this upgrade strategy is not followed	DHCP packets which previously transitioned the network without issue may now be lost if using ERS

Table continues…

	switches which utilize mixed agent versions with and without this fix.
Workaround if this upgrade strategy is not followed	• 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. • 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.

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

Effects of Upgrade on SNMP Trap Notifications

Important:

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

You can use the following procedures to restore trap functionality.

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

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

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

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

To reconfigure traps, use the following EDM procedure:

1. From the Navigation tree, click **Edit**.
2. From the Edit tree, click **Snmp Server**.
3. In the work area, select the **Community** tab.
4. Create a community string— you must specify the Notify View name.
5. In the work area, select the **Host** tab to create an SNMP host— use the community you created in the previous step.

Table continues…

6. On the **Host** tab, use the **Notification** button to activate or deactivate individual traps.
7. In the work area, select the **Notification Control** tab to activate or deactivate individual traps per device.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Updating switch software

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

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

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

OR

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

See the following sections for details about updating switch software:

- General software upgrade instructions on page 44
- Changing switch software in ACLI on page 44
- Changing switch software in EDM on page 46

General software upgrade instructions

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

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

Changing switch software in ACLI

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

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

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

3. Press `Enter`.

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

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

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

Important:

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

Job aid—download command parameters

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

Table 5: ACLI download command parameters

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

Table continues…

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

Changing switch software in EDM

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

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

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

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

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

Important:

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

Job aid—File System screen fields

The following table describes the File System screen fields.

Table 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: • IPv4 • IPv6
BinaryConfigFileName	Indicates the binary configuration file currently associated with the switch. Use this field when you work with configuration files; do not use this field when you download a software image.
BinaryConfigUnitNumber	When in standalone mode, and loading a binary configuration file that was created from a stack, this object specifies the unit number of the portion of the configuration file to be extracted and used for the standalone unit configuration. If this value is 0, it is ignored.
ImageFileName	Indicates the name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.
FwFileName (Diagnostics)	The name of the diagnostic file currently associated with the switch. If needed, change this field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	Indicates the unit number of the USB port to be used to upload or download a file. A value of 0 indicates download is via TFTP; a value of 9 indicates a standalone switch and a value of 10 indicates SFTP* server.
Action	This group of options represents the actions taken during this file system operation. The options applicable to a software download are • dnldConfig: Download a configuration to the switch.

Table continues…

Field	Description
	• dnldConfigFromSftp: Download a configuration to switch from the SFTP Server*. • dnldConfigFromUsb: Download a configuration to switch using the front panel USB port. • dnldFw: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwFromSftp: Download a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image*. • dnldFwFromSftpNoReset: Download a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset*. • dnldFwFromUsb: Download a new diagnostic software image to the switch from the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwNoReset: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • dnldImg: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. • dnldImgFromSftp: Download a new software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image*. • dnldImgFromSftpNoReset: Download a new software image to the switch from the SFTP server. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset*. • 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.

Table continues…

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

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

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

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

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

The following table describes the ip.cfg file parameters:

Table 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

Table continues…

Parameter	Description
Gateway <*xx.xx.xx.xx*>	Specifies the default gateway. Example: 181.30.30.254
SNMPread <*string*>	Specifies the SNMP read community string. Example: public
SNMPwrite <*string*>	Specifies the SNMP write community string. Example: private
VLAN <*number*>	Specifies the management VLAN-ID. Example: VLAN 1
USBdiag <*string*>	Specifies the file name of the diagnostic image to load from the USB device. Example: 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 and SFP transceiver compatibility

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
Small Form Factor Pluggable (SFP) transceivers			
1000BASE-SX SFP	850 nm LC connector	5.0.0	AA1419013-E5
1000BASE-SX SFP	850 nm MT-RJ connector	5.0.0	AA1419014-E5
1000BASE-LX SFP	1310 nm LC connector	5.0.0	AA1419015-E5
1000BASE-CWDM SFP	1470 nm LC connector, up to 40 km	5.0.0	AA1419025-E5
1000BASE-CWDM SFP	1490 nm LC connector, up to 40 km	5.0.0	AA1419026-E5
1000BASE-CWDM SFP	1510 nm LC connector, up to 40 km	5.0.0	AA1419027-E5
1000BASE-CWDM SFP	1530 nm LC connector, up to 40km	5.0.0	AA1419028-E5
1000BASE-CWDM SFP	1550 nm LC connector, up to 40 km	5.0.0	AA1419029-E5
1000BASE-CWDM SFP	1570 nm LC connector, up to 40 km	5.0.0	AA1419030-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 40 km	5.0.0	AA1419031-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 40 km	5.0.0	AA1419032-E5
1000BASE-CWDM SFP	1470 nm LC connector, up to 70 km	5.0.0	AA1419033-E5
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

Table continues…

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
1000BSE-T SFP	Category 5 copper unshielded twisted pair (UTP), RJ-45 connector	5.0.0	AA1419043-E5
1000BASE-SX DDI SFP	850 nm DDI LC connector	5.2.0	AA1419048-E6
1000BASE-LX DDI SFP	1310 nm DDI LC connector	5.2.0	AA1419049-E6
1000BaseXD DDI SFP	1310nm LC connector	5.4.0	AA1419050-E6
1000BaseXD DDI SFP	1550nm LC connector	5.4.0	AA1419051-E6
1000BaseZX DDI SFP	1550nm LC connector	5.4.0	AA1419052-E6
1000BaseCWDM SFP	1470nm LC connector, up to 40km	5.4.0	AA1419053-E6
1000BaseCWDM DDI SFP	1490nm LC connector, up to 40km	5.4.0	AA1419054-E6
1000BaseCWDM DDI SFP	1510nm LC connector, up to 40km	5.4.0	AA1419055-E6
1000BaseCWDM DDI SFP	1530nm LC connector, up to 40km	5.4.0	AA1419056-E6
1000BaseCWDM DDI SFP	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

Table continues…

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

Table continues…

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
10GBASE-ZR/ZW XFP	1550 nm SMF LC connector	5.1.0	AA1403006-E5
10GBASE-LRM XFP	1310 nm, up to 220 m over MMF, DDI	5.2.0	AA1403007-E6
10 Gigabit Ethernet SFP+ Transceivers			
10GBASE-LR SFP+	1–Port 10 Gigabit-LR SFP + (LC) Single mode up to 10 km	5.6.0	AA1403011–E6
10GBASE-ER SFP+	1–Port 10 Gigabit-ER SFP + (LC) Single mode up to 40 km	5.6.0	AA1403013–E6
10GBASE-SR SFP+	1–Port 10 Gigabit-SR SFP + (LC) Multi-mode fibre up to 300 m	5.6.0	AA1403015–E6
10GBASE-LRM SFP+	1–Port 10 Gigabit-LRM SFP+ (LC) Multi-mode fibre up to 220 m	5.6.0	AA1403017–E6
10GDAC-10M SFP+	SFP+ direct attach cable 10 m	5.6.0	AA1403018–E6
10GDAC-3M SFP+	SFP+ direct attach cable 3 m	5.6.0	AA1403019–E6
10GDAC-5M SFP+	SFP+ direct attach cable 5 m	5.6.0	AA1403020–E6
10GBASE ZR/ZW SFP+	1550 nm 80km SMF	5.8.0	AA1403016-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 supported in Release 5.8.

Standards

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

- IEEE 802.1 (Port VLAN, Port & Protocol VLANs, VLAN Name, Protocol Entity)
- IEEE 802.1AB (Link Layer Discovery Protocol)

- IEEE 802.1aq (Shortest Path Bridging)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Trees)
- IEEE 802.1v (VLAN Classification by Protocol and Port)
- IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)
- IEEE 802.1X (EAPOL)
- 802.1X-2004 (Port Based Network Access Control)
- IEEE 802.3 (Ethernet)
- IEEE 802.3ab (1000BASE-T)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10Gb/s Ethernet)
- IEEE 802.3ae (10GBASE-LR/SR/LM)
- IEEE 802.3af (Power over Ethernet)
- IEEE 802.3at (Power over Ethernet)
- IEEE 802.3u (100BASE-FX)
- IEEE 802.3u (100BASE-TX)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (1000BASE-SX)
- IEEE 802.3z (1000BASE-x)
- IEEE 802.3z (Gigabit Ethernet over Fiber-Optic)
- IEEE P802.3ak (10GBASE-CX4)

RFCs

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

Chapter 4: Resolved issues

Use the information in this section to learn more about issues that have been resolved from Release 5.7 to 5.8.

Reference number	Description
wi01162830	**EAP+SPBM**: ADAC configuration is applied correctly and the ports are assigned to voice VLAN.
wi01164355	The ND inspection for a port does not get disabled when ND dynamic learning is disabled.
wi01119064	**SPBM and DHCP Snooping/Dynamic ARP Inspection/IP Source guard:** DHCP Snooping, Dynamic ARP Inspection and IP Source guard are supported on CVLAN.
wi01133641	**MAC Security and SPBM:**The user cannot install mac-security on the NNIs, because client devices must not be connected to NNI ports. An error message is displayed if the user attempts to enable mac-security on all the ports on the stack using a port-range.
wi01115661	**802.1x trace support:** If trace is enabled, maximum number of EAPOL clients can be reached.
wi01161975	The RW/RO passwords do not get corrupted when the switch is downgraded from Release 5.8 to 5.7.
wi01136677	**ACLI, show port information:** The last status change timestamp information for port configurations is available in the ACLI show commands (that is the **`show interfaces`** command).
wi01130870	**EAP+SPBM:** EAP/NEAP configuration is supported on SPBM enabled switch or stack.
wi01132847	**SPBM:** MAC Security DA filtering is supported on SPBM CVLAN ports.
wi01133635	**AUR:** When autosave is set to disabled, the stack units transition back to Ready for Replacement state. The command **`show stack auto-unit-replacement`** displays the units are ready for replacement.
wi00960581	**ERS 4800, RADIUS Management Logging**: When a telnet connection is made to ERS 4800 switch operating in standalone mode, the NAS-Type-Port is Ethernet.
wi00928249, wi00928260	**ERS 4800, Stack Statistics:** On ERS 4800 models, the multicast or broadcast packet statistics are incremented and displayed in the **`show stack port-statistics`** command output.
wi00841955	**802.1AB MED, Auto QoS:** The LLDP MED network policy configuration does not change when there is a custom LLDP MED policy and Auto QoS is enabled.

Table continues…

Reference number	Description
wi00900220	**Port Mirroring, XrxYtx:** In XrxYtx port mirroring mode, broadcast traffic is correctly mirrored to the monitor port.
wi00850597,wi00850936,wi00850590	**802.1AB Integration / Power Conservation:** If the switch sets the power conservation TLV to zero (indicating that no power conservation must be used by the IP Phone), Avaya 9600 IP Phones return 0 value.

Chapter 5: Known Issues and Limitations

Use the information in this section to learn more about known issues and limitations from Release 5.7 to 5.8. Where appropriate, use workarounds provided for the known issues and limitations.

Known Issues and Limitations for Release 5.8

The following table lists known issues and limitations for Software Release 5.8.

Reference number	Description
wi01170561	**PIM-SM**: After the user stops sending source items, the source, group (S,G) entries are not deleted from the Session Detail Records (SDR) to Rendezvous-point (RP) path.
wi01168385	**EAP+SPBM**: Some NEAP clients from Temporary Base Unit (TBU) are not authenticated after they bounce user-based policy (UBP) support level.
wi01132037	**Change RADIUS Passwords on EDM**: According to the modified policy, the new password must be different from the last five used. While changing the RADIUS password in EDM, you can select an old password from the previous five passwords.
wi01134313	**MAC Address Table**: When MAC addresses are sent on multiple ports at a cumulative rate, all MAC addresses may not appear in the MAC address table. This causes unreliable basin switch functionality. **Workaround**: You can shut/ no shut the ports where the MAC addresses are not learned.
wi01143005	**No MHMV support in conjunction with SPBM**: In Release 5.8, Multiple Hosts with Multiple VLANs (MHMV) are not supported in conjunction with SPBM.
wi01161383	**Lockout for failed login attempts**: For RADIUS and TACACS authentication, the lockout feature does not work for failed login attempts.
wi01152139	**Using EAP in a SPBM environment**: Block Subsequent MAC Authentication does not work after reset. **Workaround**: It is recommended to use only EAP or NEAP clients on a port when Block Subsequent MAC Authentication is enabled.
wi01147948	Log messages are not generated when port assignment into RAV fails. **Workaround**: It is recommended not to use EAP in conjunction with switched UNI VLANs.

Known Issues and Limitations for Releases Prior to Release 5.8

The following section lists known issues and limitations in Avaya Ethernet Routing Switch 4000 Series software which are present in Release 5.8 and are also known to be present in older releases of the software.

Table 10: Known issues and limitations

Reference number	Description
wi01134550	**RADIUS:** After changing the RADIUS password in EDM, if you open a new EDM session in a different browser, an error message can appear in the second browser when trying to connect to EDM.
wi01103905	**SPBM Cloud:** Addresses learned over SPBM cloud can sometimes be displayed in CAM with a delay of 20 seconds.
wi00950753	**EDM, QoS, Traffic Profile Committed Rate**: When you configure Traffic Profile set, the committed burst size value is different for EDM and ACLI configuration for the same committed-rate and max-burst-rate.
wi00989636	**ERS 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+, 4550T-PWR+, 4526T-PWR+, Minimum Software Revision:** The minimum software revision for 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+, 4550T-PWR+, 4526T-PWR+ is 5.6.0. The minimum software revision for 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+, 4550T-PWR+, 4526T-PWR+ with hardware revision 10 or later is 5.6.1. **Warning:** Attempting to downgrade the software to release 5.6.0 or earlier on an Ethernet Routing Switch 4500-PWR+ or 4800 (hardware revision 10 or later) will render the unit inoperable.
wi01135697	**Change RADIUS password**: When the RADIUS server is set with the option that the user cannot change the password, the telnet or ssh sessions do not display the error message when you try to change the password for a user. However, CLI session displays the correct Access-Reject (E=709) error message.
wi01112965 wi01113343	**802.1x NEAP Not Member of VLAN:** For all NEAP RADIUS clients that try to initially authenticate a port unassigned to any VLAN, only RADIUS assigned VLANs from STG1/CIST are supported.
wi01113962	**MAC Security Lockout Port:** The MAC Address table lists the MAC Addresses even when the mac-security lockout is enabled on non-base unit (NBU) port. **Workaround:** Configure mac-security lockout ports and then, configure MAC security settings.
wi01113653	**MAC Security Lockout Port:** When ports previously configured with mac security are included in the mac security lockout list, traffic still follows the filtering policy of mac security. **Workaround:** Configure the mac-security lock out ports and then configure mac security settings.

Table continues…

Reference number	Description
wi01081726	**ISIS:** The ISIS CSNP-interval does not affect generating CSNP. CNSP is generated only after the adjacency is established. All other ISIS packet types such as LSP and PSNPs are generated and received on adjacent devices. **Note:** ERS 4000 does not support multi-access networks with designated routers. ERS 4000 release 5.7 supports only point to point interfaces.
wi01101547	**SPBM:** SPBM cannot be enabled when Autosave is disabled.
wi01078500	**SPBM:** Do not use multiple redundant links between two SPB devices if multiple interfaces do not belong to a MLT.
wi01081438	**SPBM:** On ERS4xxx platform, if multiple VLAN are mapped to same ISID, traffic is forwarded to all VLANs.
wi01081961	**SPBM:** COM 3.0.1 and VSN Manager, which is the feature/component of COM, do not support 4xxx platform.
wi01075348	**SPBM:** NNI VLAN settings are not restored after ISIS is disabled.
wi01076939	**SPBM:** No log message is generated when ISIS authentication mismatch occurs.
wi01082763	**SPBM:** SPBM instance can not be created using EDM offbox.
wi01083290	**SPBM:** No log message is generated when adjacency between two SPB devices fail due to b-vlan mismatch.
wi01085468	**SPBM:** Unknown multicast allow flood does not work on CVLAN.
wi01115016	**SPBM:** ISIS is disabled on Non Base Units which are removed from stack.
wi01101543	**SPBM MLT/DMLT configuration from EDM/EDM offbox (COM):** All MLT/DMLT members of an ISIS interface are displayed into EDM/EDM offbox as separate ISIS interfaces in addition to the original ISIS interface corresponding to the MLT/DMLT. In ACLI, only the ISIS interface corresponding to MLT/DMLT interface is displayed.
wi01101846	**SFTP Enhancement for "license and DHCP Snooping external save " configuration from EDM offbox:** Response timeouts may appear in EDM when copying the license file from the SFTP server. It is recommended to use a 20 seconds timeout for the EDM offbox (COM), to avoid EDM response timeouts. **Workaround:** Use ACLI to copy the license file.
wi01120630	**Fail Open VLAN:**After defaulting the RADIUS server IP address, EAP clients might remain authenticated. Defaulting the RADIUS server IP address should be avoided when EAP/NEAP clients are assigned into Fail Open VLAN.
wi01124666	**SFTP Enhancement for "license and DHCP Snooping external save " configuration from EDM offbox:** Response timeouts may appear in EDM when performing SFTP-related configurations. **Workaround:** It is recommended to use a 20 seconds timeout for the EDM offbox (COM).
wi01127487	**EDM:** Some EDM tabs may be not accessible from Internet Explorer 9 and Internet Explorer 10.

Table continues…

Reference number	Description
	Workaround: Use the compatibility mode view in Internet Explorer versions 9 and 10 to correctly display EDM.
wi01129281	**USB:** The USB stick may be not recognized after hardware or software reset. **Workaround:** Remove and reinsert the USB stick in the USB port to make it accessible. In some cases, a reset may be needed.
wi01133518	**SPBM:** When the management VLAN is configured as CVLAN, the **`show arp-table`** command does not display the MAC-IP address ARP entry of the default gateway. The ARP entry is learned and used by the switch or stack, even if it is not displayed.
wi01114629	**SPBM:** Response timeouts may appear when using the **`show mac-address-table`** command or SPBM-related commands immediately after switch reset. It is not advisable to issue SPBM related commands or **`show mac-address-table`** command until reboot is fully complete. **Workaround:** Wait 4 minutes after the units have joined the stack.
wi01075599	**SPBM and port mirroring:** Port mirroring is not supported on the NNI ports.
wi01102653	**SPBM:** IPv6 management is not supported on the management ISID.
wi01133906	**SLA Mon:** RTP timers are displayed in EDM in microseconds instead of milliseconds.
wi01046652	**802.1X, EAP, NEAP, RAV, Different Spanning Tree Group:** When the RADIUS Assigned VLAN (RAV) for a port is in a different Spanning Tree Group to the previous VLAN assigned to the port, the RAV will not be applied. **Workaround:** It is recommended to use same Spanning Tree Group for all EAP related VLANs: Guest, FailOpen, EAP voice vlan, initial VLAN and RADIUS Assigned VLAN (RAV).
wi01048962	**802.1X, Fail_Open Continuity Mode:** You can configure Fail_Open Continuity Mode when the Fail_Open VLAN is disabled. **Workaround:** It is recommended to enable Fail_Open Continuity Mode only when Fail Open VLAN is enabled.
wi01042215	**802.1X, MHSA, Multi-VLAN:** If you attempt to configure Multi-VLAN when MHSA is also configured on the switch, the show command "show eapol multihost status" may take a long time to display output. **Workaround:** Customers are advised that Multi-VLAN operation should not be configured in conjunction with MHSA.
wi01048958	**802.1X, NEAP, Multi-VLAN, Fail_Open Continuity Mode:** NEAP clients may incorrectly remain authenticated after the re-authentication-period expires if the switch is setup to use NEAP RADIUS Server and Multi-VLAN is disabled on the port. **Workaround:** It is recommended to enable Multi-VLAN if Fail Open Continuity Mode is enabled and different Radius Servers are configured.

Table continues…

Reference number	Description
wi01047064	**802.1X, User Based Policies, EPM:** User Based Policies (UBP) must be defined locally on the switch/stack, as this implementation does not support the dynamic download of policies from Enterprise Policy Manager (EPM).
wi01060151	**802.1X, User Based Policies, EDM:** EDM does not provide the ability to set User Based Policies or User Based Policies for NEAP with this release. **Workaround:** The CLI can be used to configure these settings.
wi01035352	**802.1X, User Based Policies, Filter on MAC, MHSA:** If the switch port is setup for MHSA, a NEAP client authenticated after EAP device will not have the User Based Policies (UBP) filter on MAC applied to the port.
wi01037828	**802.1X, User Based Policy, Change Security Level:** If you change the User Based Policy (UBP) security level from high to low while clients are authorised, the high security filter will remain in place until clients are reauthorized. **Workaround:** To enable connected users policy to be updated, set the port to reauthorize after changing UBP security mode to low.
wi01048480	**EAP, Unable to Change Port Authorization State:** In a situation where all QoS precedences are used on the switch, it may be impossible to change the EAP port authorisation status from auto to unauthorized. **Workaround:** Change EAP port state from auto to authorized and then to unauthorized.
wi01003809	**802.1X/EAP, Syslog:** The following error message may be incorrectly generated for EAP "EAP Error Radius - ifIndex not found port 0".
wi00978985	**ASCII Script Table:** A General failure message may occur when configuring an ASCII script entry with filename of greater than 30 characters. **Workaround:** Switch operation is otherwise not affected, specify filename of 30 characters or less when using ASCII script table.
wi00987130	**EAP Trace:** Trace configurations are dynamic and not saved across switch resets. Thus if you have Trace enabled in a stack and you reset one of the units within the stack, then after reset, the unit will no longer be performing trace function. **Workaround:** Reconfigure trace level setting after the unit is reset.
wi01000089	**MAC Filtering, Maximum VLANs:** If a configuration consisting of multiple MAC DA filter entries per VLAN with maximum number of VLANs, it is possible that the MAC FDB may be filled resulting in no space for additional MAC entries. **Workaround:** Ensure that the number of MAC DA filter entries multiplied by the number of VLAN configured on switch/stack is less than 8,192 entries.
wi01002073	**NTP, Statistics:** When NTP authentication is enabled**,** NTP statistics are incorrectly displayed.
wi01009029	**Protocol VLAN, Tagged Ports, Changed Operation:** In previous software release, if the ingress port was tagged, classification would be based on the PVID and not on the ingress packets Ethertype. The operation for Protocol VLANs has been updated to operate correctly for tagged port, such that VLAN membership will be determined first by the Ethertype on tagged ports.
wi00978033	**Running Configuration, Shared-ports:** The shared port commands are not output by the show running-config command or in the ASCII configuration.

Table continues…

Reference number	Description
wi00980989	**Shared-port s, Speed/Duplex:** Setting the speed/duplex parameter on a port with shared-port force is not supported.
wi00995946	**Software Downgrade, Configuration Reset:** When downgrading 5.6.1 image to 5.4 or earlier, both configuration NVRAM blocks will be defaulted. This is operation. **Workaround:** If the configuration is required on downgrade, the customer should save the configuration to ASCII and then restore this once the downgrade to 5.4. or earlier software has been completed.
wi01005690	**SSH client, SNMP:** If querying the switch SSH Client parameters via SNMP, the value returned by rcSshcGlobalRsaAuthentication is incorrect, you should use the SNMP object rcSshcGlobalRsaAuthenthication.
wi00991539	**USB:** The Ethernet Routing Switch 4000 does not support USB sticks/drives formatted as NTFS. **Workaround:** Use USB sticks/drives formatted as FAT32 or FAT.
wi00897222	**802.1AB (LLDP)**: If displaying the status for LLDP dot1 transmission flags in a stack which have 1024 VLANs configured, this will take considerably longer if you use the console port of a Non-Base Unit in the stack. **Workaround**: Avaya recommends that you perform all configuration and display using the console port on the Base Unit of a stack.
wi00887780	**Brouter Ports**: When you create brouter ports, if the maximum number of IP interfaces is reached, the following message will be displayed in ACLI: `%Maximum IP interfaces are already configured`. In this case the system will not create the brouter port, however the port may be removed from the initial VLAN if VLAN configcontrol is set to automatic and that port will then be without VLAN membership. **Workaround**: To reactivate the port, add the port to the desired VLAN and re-enable STP participation for that port as appropriate.
wi00888620	**Brouter Ports**: Avaya recommends that you do not renumber units if brouter ports are used. This may result in routes being improperly deactivated and in loss of connectivity. **Workaround**: If it is necessary to renumber the stack, you should remove brouter ports, renumber the stack and then recreate brouter ports.
wi00944306	**Brouter Port, MSTP**: If you attempt to configure a brouter port on a port which is assigned to a VLAN configured in MSTI when running in MSTP mode, then the operation will not be applied. **Workaround**: If using MSTP mode, move the port to a VLAN which is a member of CIST then perform the brouter port assignment.
wi00949343	**Brouter Port, STP**: By design, STP participation is disabled when a brouter port is configured. If you then delete the brouter port, STP participation remains disabled on that port. **Workaround**: Re-enable spanning tree on the port if required after a brouter port instance is deleted.
wi00946493	**DHCP Snooping Option 82**: When DHCP Snooping is configured with Option 82 support and both the DHCP server (trusted port) and the DHCP client are on the base unit of a stack, then the option 82 information will not be added to the DHCP release packet or the DHCP unicast requests that the client generates. **Workaround**: Locate the DHCP server or trusted uplink ports on a port which is not on the base unit.

Table continues…

Reference number	Description
wi00939421	**EDM, IP Phone Automatic PoE Changes**: When IP Phone Automatic PoE Changes is enabled, the dynamic power limit or dynamic power priority is not displayed in EDM. **Workaround**: Use ACLI to query PoE priority and limits when IP Phone Automatic PoE is configured.
wi00928161	**EDM, PoE Status**: In EDM PoE ports may display an incorrect status of `otherFault` instead of `Deny Low Priority`. **Workaround**: Use ACLI to display the correct PoE status information
wi00939773	**EDM, SFTP**: If you use SFTP with password authentication enabled and you do not configure a password, no warning message will be generated by EDM and the SFTP operation will fail. **Workaround**: Ensure that you configure a password in EDM for SFTP if the SFTP authentication type is set to password.
wi00896456	**ERS 4800, 4500-PWR+**: When you add an ERS 4800 or 4500-PWR+ unit to an existing stack, that stack must be running 5.6.0 or later release software. If the stack is running an earlier software release, the switch will not be allowed to join the stack as the software on these new models cannot be downgraded to releases prior to 5.6.0. **Workaround**: First upgrade the existing stack to the 5.6.0 or later software. Then add the ERS 4800 or 4500-PWR+ unit to the stack. Alternatively you could add the ERS 4800 or 4500-PWR+ unit as the new base unit to the stack; remembering only one unit in the stack can have the Base Unit switch set to on.
wi00945097	**ERS 4800, TDR**: When performing the TDR function on an ERS 4800 switch, the switch will incorrectly report swapped pairs for a straight through cable.
wi00945147	**ERS 4800, TDR**: When performing the TDR function on an ERS 4800 switch, if the switch is connected to an ERS 4500, then the switch will incorrectly report that pairs 1 and 4 are inverted.
wi00936995	**IGMPv3**: If the size of the IGMPv3 membership report is greater than 1600 bytes, the membership report will not be processed by the switch. IGMPv3 membership reports may contain join requests for multiple groups in one request. **Workaround**: Limit the maximum number of multicast groups per join request to less than 195 groups.
wi00959759	**IGMPv3, Maximum Entries** : The maximum number of IGMP groups learned by IGMP Snooping on the switch is 512. However, this depends on the hardware table usage. With IGMPv1/v2 there is a direct correlation between the number of groups and entries. IGMPv3 on the other hand may use more than one hardware entry per group. An IGMPv3 group with N source addresses will typically consume N+1 hardware entries. As an example an IGMPv3 group with 2 specified source will use 3 hardware entries.

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

wi00894579	**IGMP, Multicast Flood, OSPF**: If you configure IGMP Snooping with the unknown multicast no flood option, the system drops control traffic for protocols that use

Table continues…

Reference number	Description
	multicasting (example, OSPF). **Workaround**: Configure unknown multicast allow flood specifically for the required multicast group.
wi00934434	**IP Phone Automatic PoE Changes, Energy Saver**: If Energy Saver has been configured for PoE power savings mode, then it will not take into account the dynamic PoE priority of a port which is allocated through the IP Phone Automatic PoE function. Thus if the underlying static PoE priority is low and even though the IP Phone Automatic PoE has set a port to high or critical PoE priority, energy saver will power down the port if poe-saver is enabled when energy saver activates. **Workaround**: Avaya recommends not to use poe-savings mode in combination with IP Phone Automatic PoE changes with this release.
wi00929526	**IP Routing, Route Summary Display**: When performing the **`show ip route summary`** command, the number of connected routes is incorrectly displayed as 0. **Workaround**: Use the command **`show ip route`** and if necessary perform a count of the directly connected routes.
wi00894103	**NTP**: You can enable NTP without configuring an NTP server, which will result in no time synchronization. **Workaround**: You should configure at least one NTP server for synchronization to occur.
wi00895539	**NTP, IPv6**: NTP does not support the configuration of servers using IPv6 addressing with this release.
wi00934809	**MAC Address Table, Layer 2 FDB**: With the introduction of new features such as static MAC addresses with this release, the MAC addresses of each of the units in the stack will now be shown in the MAC Address table or Layer 2 Forwarding Database (FDB). This is an expected operation and no action is required on your part.
wi00962297	**PoE+ Firmware**: In some cases it may be necessary to upgrade the PoE+ firmware on PWR+ models. In some cases if you attempt to perform a PoE+ firmware update on a stack of 8 units, the update may fail. The download will always succeed if there are 7 or less PWR+ units in a stack. **Workaround**: Reset the stack and attempt to reload the PoE+ firmware or remove one unit from the stack and re-download the PoE+ firmware.
wi00933497	**Port Mirroring, Ingress & Egress Mirroring**: When you use port mirroring, if a packet is both ingress and egress mirrored, two copies of the packet will be sent to the MTP ports. If the egress port is operating in tagged mode, then one copy of the packet will be untagged and another copy of the packet tagged from the egress port. This is expected operation.
wi00955218	**Port Mirroring, XrxYtx, IP Routing**: When performing port mirroring in XrxYtx mode on an ERS 4500 switch, traffic which is to be routed will not be mirrored; this is a hardware limitation. When performing port mirroring in XrxYtx mode on an ERS 4800 switch, traffic which is to be routed will be correctly mirrored to the mirror to port.
wi00950622	**QoS, Queue Shaping**: If queue shaping min rate is configured on the highest queue number, then in an oversubscription scenario this rate may not be fully respected if it exceeds 98% from egress bandwidth.
wi00958103	**QoS, Strict Priority, WRR Algorithm**: The ERS 4800 will process traffic differently to ERS 4500 switches when egress queues are congested. On an ERS 4800

Table continues…

Reference number	Description
	switch, during periods of congestion, low drop precedence traffic will be buffered, while high drop precedence traffic could be dropped if there is insufficient egress buffers available
wi00939391, wi00939393	**Shared Port, SFP**: New shared port functionality using the **`shared-port auto-select`** command may not work correctly on models other than the 4526GTX, 4526GTX-PWR, 4548GT and 4548GT-PWR.
wi00959035	**SFP, Display**: If AA14190040 or AA1419029 CWDM SFPs with the vendor ID of OCP are installed in the switch, a **`show interfaces`** or **`show gbic-info`** will incorrectly display these devices as operating at 100Mbps instead of 1Gbps.
wi00859047	**SSH**: The CLI command **`show ssh download-auth-key`** does not display the last transfer result when you download the key from USB. **Workaround**: If the download of the SSH key was successful, then when you display the ssh or sshc status you will see the key has been loaded by the switch. Alternatively loading the SSH key from a TFTP server will display the correct result.
wi00959582	**SSH, DSA/RSA Key Length**: When you upload the DSA/RSA key to a TFTP server or USB device from a switch/stack you can generate a filename with up to 128 characters. When you attempt to download the DSA/RSA keys, the switch supports a maximum of only 30 character filenames. **Workaround**: Avaya recommends you use filenames with a maximum of 30 characters for DSA/RSA keys.
wi00891090	**SSH Client, Break Sequence, Syslog**: When you use the SSH client from the switch or stack, if you terminate a server connection with the "~." break sequence, the system does not generate a `SSH disconnected` syslog message.
wi00894057	**Voice VLAN, 802.1AB (LLDP)** : When you can create a LLDP MED network policy there is no check performed to ensure that the VLAN type is set to Voice. **Workaround**: Ensure that you configure the VLAN appropriately as a Voice VLAN before setting the LLDP MED network policy.
wi00893827	**Voice VLAN, ADAC, EAP**: Avaya recommends you do not use the same VLAN ID for ADAC Voice VLAN and EAP Voice VLAN.
wi00930645	**Voice VLAN, 802.1AB (LLDP) MED Policy**: When you configure a VLAN as type Voice, you will still need to explicitly configure 802.1AB (LLDP) MED Network policy to advertise that VLAN via LLDP to end devices.
wi00868382, wi00554875	**802.1AB / LLDP Default Parameters, ADAC**: In Software Release 5.5, 5.6 and later with the introduction of 802.1AB default parameters a default LLDP MED policy is configured on all ports. The default values for that policy are as follows: application type = voice, tagging = untagged, DSCP = 46 and VLAN priority = 6, VLAN id= 0. If ADAC is configured on that port and an IP Phone is detected, the dynamic LLDP MED policy will not be installed, resulting in the IP phone not receiving the correct VLAN configuration if ADAC tagged frames is used. This happens because the default MED policy is static and overrides the dynamic policy installed by ADAC. **Recommendation**: If ADAC is to be used, then it is recommended that the default 802.1AB/LLDP MED policies are deleted on telephony ports and on uplink/call

Table continues…

Reference number	Description
	server ports. Use the interface command **`no lldp med-network-policies`** on telephony ports and on uplink/call server, prior to configuring ADAC on ports.
wi00863027	**802.1AB Default Values**: When you upgrade to 5.5 or 5.6 software, any old 802.1AB values will be maintained. The new default 802.1AB values are only applied if you reset the configuration (for example, use the **`boot default`** command).
wi00856869	**802.1AB Integration / ADAC**: Avaya IP Phones will perform a reset when connecting to the switch if 802.1AB Integration (use of 802.1AB TLVs) is enabled in conjunction with ADAC. **Workaround**: Create a manual 802.1AB-MED network policy which will then change the order in which information is supplied to the IP Phones.
wi00858022	**802.1AB Integration / Avaya IP Phone**: When the switch detects an Avaya IP Phone, it sends four LLDP packets (according to MedFastStartRepeatCount). With some models of Avaya IP Phone, this process is repeated 60 seconds after device detection. **Workaround**: None required.
wi00861373	**802.1AB Integration / Call Server TLV**: An IP Phone may incorrectly report the Call Server in-use IP address to the switch if different call-servers were previously configured and cached by the IP Phone. **Workaround**: If it is found that there is a mismatch of in-use call-server addresses cached by the IP Phone, then performing two consecutive resets of the IP Phone will clear the incorrect data from the IP Phone cache and result in correct information being returned to the switch.
wi00861372	**802.1AB Integration / Call Server TLV**: You can configure up to 8 Call Server IP Addresses on the switch for maximum resiliency. When some of the Call Servers are unreachable, the Avaya IP Phone may incorrectly indicate to the switch that it is using one of the unreachable Call Servers. **Workaround**: Information on call server use can be obtained from the phone or the call server.
wi00855650	**802.1AB Integration / SIP Configuration**: The currently defined Avaya Proprietary TLVs, do not support the direct provisioning of SIP parameters (transport protocol, port number, domain name) from the switch to the IP Handset. **Workaround**: The SIP information can be supplied to the IP Phone through the configuration file server, ensure that the File Server TLV is appropriately configured.
wi00841065	**802.1AB MED Network Policy**: When upgrading to 5.5 or 5.6 software and the previous configuration contained no network policies, the new default network policies will be applied.
wi00484050	**ACG, SNMPv3, Secure Image**: When you run the secure software image, an ASCII configuration file generated by the switch has the SNMPv3 user commands **`snmp-server user`** commented out. This is expected behavior as the associated passwords cannot be output in clear text in the ASCII generated file due to security requirements. As a result when the configuration is loaded onto a switch with default configuration, the SNMPv3 users are not recreated. **Workaround**: Manually recreate the SNMPv3 users after loading the ASCII configuration.
wi00491471	**ADAC, EAP, Guest VLAN**: If you configure both Guest VLAN (GVLAN) and ADAC untagged frames advanced mode on a port, then when a device is discovered by ADAC the port is moved from the GVLAN into the ADAC Voice VLAN. This results in lost connectivity for the GVLAN. If you disable ADAC globally, the client is

Table continues…

Reference number	Description
	removed from the ADAC Voice VLAN and placed in the initial port based VLAN with the PVID set to 1 (the default VLAN). **Workaround**: Avaya recommends you do not use ADAC untagged frames advanced mode in combination with EAP MHMA and Guest VLAN.
wi00932189	**DHCP Snooping External Save, USB, Stack Renumbering**: If you have DHCP Snooping External Save configured to save the database to a USB drive on a particular unit, then if you perform a stack renumbering the feature may incorrectly point to the USB device on the wrong unit. **Workaround**: If you have DHCP Snooping External Save configured to save the database to a USB drive, then after performing a stack renumbering you should re-configure DHCP Snooping External Save to use the renumbered unit in which the USB devices is located.
wi00484170	**EAP, 384 ports, Intruder MAC**: If you enable or activate EAP on 384 ports simultaneously, while all clients are sending large volumes of traffic, then some intruder (unauthorized) MAC addresses may not appear in the MAC address table. This applies only to intruder addresses which are blocked and not allowed to forward traffic and it is not a security or connectivity problem.
Q01981920	**EAP, Fail Open VLAN**: An EAP or Non-EAP client could be assigned to the Fail Open VLAN in normal operation if the VLAN name or ID returned from the RADIUS server matches the VLAN assigned for the Fail Open VLAN. **Workaround**: Ensure that the Fail Open VLAN name or ID that you use does not match one of the returned RADIUS VLANs.
wi00491652	**EAP, Guest VLAN**: If you disable Guest VLAN (GVLAN) globally or per interface while authenticated clients are present, the system does not remove the port from the GVLAN. **Workaround**: It is recommended that you shut down the switch port before you disable GVLAN, either globally or per interface. Shutting down the port clears the authenticated clients so that the ports are correctly removed from the GVLAN.
wi00484217	**EAP, MHMA MultiVLAN, Guest VLAN** : Switch ports are not moved into the Guest VLAN (GVLAN) if you enable the GVLAN option after EAP clients have authenticated on the port. **Workaround**: It is recommended that you enable Guest VLAN (global or per port option) before EAP clients are authenticated. Alternatively, you can globally disable EAP, configure GVLAN, then re-enable EAP globally.
wi00878611	**EAP, NEAP, Fail Open VLAN**: After the RADIUS server becomes unreachable, then reachable again, not all 384 NEAP clients may be re-authenticated in some circumstances. **Workaround**: After the RADIUS server becomes reachable, you can either reboot the stack or manually clear the MAC address table on the EAP enabled ports using the interface configuration command **`clear mac-address-table interface fastEthernet <portlist>`**.
wi00491727	**EAP, QoS Traffic Profiles**: If you configure both QoS Traffic Profiles and EAP, in some circumstances after a switch reboot the QoS Traffic Profile may be set to a higher precedence than before the switch reboot. EAP packets could then be blocked by rules defined in the traffic profile. **Workaround**: To prevent EAP packet blocking in this situation, you can define a QoS policy instead of using a Traffic Profile. The same filtering capabilities are supported, but user defined policies use the same QoS precedence correctly before and after a reset.

Table continues…

Reference number	Description
wi00483818	**EAP, RADIUS Last Assigned VLAN**: When a port is configured for RADIUS Last Assigned VLAN, if the last RADIUS authentication for that port does not contain QoS priority, then the port priority will be either the one manually configured for that port or the one received for the previous authenticated client.
wi00489861	**EDM, ASCII Configuration**: When loading an ASCII configuration file using EDM it is recommended that the switch has minimal configuration changes from default. Otherwise existing switch/stack configuration might cause warning or error messages that force the ASCII configuration to exit with a FAIL status. **Workaround**: Apply ASCII configuration from EDM to a switch or stack that has a basic configuration. Alternatively, a currently-configured switch/stack can be re-configured using an ASCII configuration via CLI (console, telnet, SSH) since the system ignores warning and error messages and configuration continues until the last ASCII file line executes.
wi00906624	**EDM Help, Classifier Blocks**: The EDM help text for QoS Classifier Blocks incorrectly states that the eval order parameter can range from 0 to 65,535 when it should state 1 to 65,535.
wi00893619	**EDM, Firefox, Ipmgr blocked**: When you open EDM in Firefox on a switch/stack where the ip manager has blocked the source IP address of your browser, you will get a blank page in the Firefox browser rather than a pop-up box advising that access from your browser IP address is blocked. **Workaround**: Using IE will result in the appropriate pop-up box advising that access from your browser IP address is blocked.
wi00962126	**EDM, Memory Utilization**: The Memory utilization information which is shown in EDM may not reflect the correct values. **Workaround**: Use ACLI or SNMP to obtain the correct values.
wi00491403	**EDM, Multiport configuration**: When you use EDM to apply an operation to all ports, the system may generate a misleading error message if the change could not be applied to all ports (for example if applying a PoE setting to PoE and non-PoE ports). EDM provides only an error message indicating the first port for which it was unable to apply the configuration change.
wi00876311, wi00897706	**EDM, Script Busy**: When connecting to EDM the following message may appear: `A script on this page may be busy, or it may have stopped responding. You can stop the script now, or you can continue to see if the script will complete`. **Workaround**: Check the remember option and click the continue button from the browser and the message will no longer be displayed.
wi00841212. wi00483820	**EDM, TACACS+**: You cannot use EDM to enable TACACS+ because the system disables Web access to the switch when you enable TACACS+ via EDM. If you used EDM to enable TACACS+ you would lose EDM access for any subsequent operations.
wi00930313	**EDM, USB, Binary Configuration**: When saving a binary configuration file to a USB device, if you do not specify a Binary Config Filename, the following message is displayed which may be misleading: `No USB storage device detected`. **Workaround**: Set the binary config filename in order to save/retrieve the configuration to/from a USB device.

Table continues…

Reference number	Description
wi00846698	**EDM**: EDM multiport select does not work on interfaces with SFPs/XFPs inserted. Please use per port configuration for interfaces with optics installed.
Q02121888, Q02121890	**Energy Saver, Copper ports, RIP, OSPF**: When you activate or deactivate energy saver, the link on a port briefly transitions. This transition may cause OSPF neighbor connectivity to bounce or cause relearning of RIP routes. **Workaround**: Avaya recommends that you disable energy saver on copper uplink ports which have OSPF adjacencies or RIP routes active. Copper ports, OSPF adjacencies—If you use copper ports for which energy saver is enabled and OSPF adjacencies are exchanged over these links, you can set the ip ospf advertise-when-down enable parameter so that adjacencies are not bounced when the link transitions. Copper ports, RIP routes—If you use copper ports for which energy saver is enabled and RIP routes are exchanged over these links, you can set the ip rip advertise-when-down enable parameter so that RIP routes are not bounced when the link transitions. Alternative: If you use fiber ports for OSPF adjacencies or RIP route connections, energy saver will not cause a link transition.
wi00900252	**Energy Saver**: If you disable Avaya Energy Saver while it is in power saving mode on ports which are administratively set to 100Mbps, these ports will then operate at 10Mbps. **Workaround**: Deactivate energy saver using the **`energy-saver deactivate`** command in Privileged EXEC mode before disabling energy saver.
wi00483987, wi00484314, wi00484346, wi00491683	**Energy Saver**: When energy saver is activated or deactivated, the link on a port transitions briefly. This brief transition can cause some devices to reacquire connectivity, but, in most situations, end users do not notice the port transition. On the switch, the system clears the MAC address for the port and then relearns it. If EAP or NEAP is enabled, EAP authentication restarts. **Workaround**: Avaya recommends that you disable energy saver on copper uplink ports because activating or deactivating energy saver on copper ports triggers a link down followed rapidly by a link up event. Alternative: Use fiber ports for uplinks because energy saver does not change fiber port status when energy saver is activated or deactivated
wi00931011	**IP Source Guard (IPSG), MLT, DMLT, LAGs**: If IPSG is configured on MLT/DMLT/LAG/DLAG ports and these ports are manually shutdown, then entries may remain in the IPSG filtering table even though there are no longer any addresses associated with the port. **Workaround**: Avaya recommends that if trunk ports are likely to be regularly manually shutdown and enabled, that IPSG should not be configured on trunk ports (MLTDMLT/LAGs).
Q01979384	**IPv6**: Due to the short, or transient, nature of TCP connections for HTTP requests it is likely that IPv6 HTTP connections may not be displayed when you use the CLI command **`show ipv6 tcp connections`**. This behavior is considered normal. **Workaround**: If simultaneous Web page refresh commands are issued, then a **`show ipv6 tcp connections`** command displays the active TCP connections for the Web session.
wi00489936	**Jumbo Frames**: As the Avaya Ethernet Routing Switch 4000 supports jumbo frames (up to 9216), the Jabber counter will always be displayed as zero (0). **Workaround**: You can find information about framing errors in the etherStatsCRCAlignErrors counter.

Table continues…

Reference number	Description
wi00489794	**Link-up during boot**: During reboot or power up operations, but before the agent code loads, the switch may provide an intermittent link to devices connected to front panel ports. Regardless, no traffic switching occurs until the agent code load completes. **Workaround**: If uplinks are connected to fibre SFP/XFP/SFP+ devices then these devices will not provide link-up until the switch is fully operational.
wi00930449	**MAC Security, MLT, DMLT, LAGs**: Traffic may be incorrectly filtered if MAC security is enabled on trunk ports. **Workaround**: MAC security should not be configured on trunk ports (MLTDMLT/LAGs).
wi00483597	**Management VLAN**: When operating in Layer 3 mode, using the Management VLAN for normal routing may result in lost connectivity to the Management IP address. **Workaround**: If connectivity problems occur to the management IP address, clear the ARP cache.
Q02118229	**MIB, EAP, MHMA MultiVLAN**: If you disable the MHMA MultiVLAN option, the SNMP MIB object (bseeMultiHostStatusVid) that reports the VLAN associated with a client reports a value of either 4095 or 4096. The returned VLAN ID values of 4095 or 4096 indicate that the VLAN was not assigned to the client. This is normal, expected behavior in this scenario. Use the CLI command **`show eapol multihost status`** to confirm the VLAN ID association.
wi00848300	**NEAP, IP Phone, Multi-VLAN, ADAC**: If EAP Voice VLAN is used in combination with non-eap-phone option and ADAC is configured for tagged frames and EAP multi-vlan is enabled; then if EAP is disabled after IP Phone is detected and authenticated the PVID of the port is reset to the initial value instead of remaining equal to the value set by ADAC. **Workaround**: Perform a poe shutdown and then no poe shutdown on the IP Phone port so that the Phone is rediscovered and the PVID is set accordingly.
wi00863853	**NEAP, Multiple Requests:** If the switch is operating with more than 1 NEAP client per port and you issue the **`clear mac-address-table`** or **`clear eapol non-eap`** command, then the switch sends multiple consecutive access-request for the same NEAP client, during the same authentication session.
Q01977243	**QoS information**: Non QoS applications, such as UDP Forwarding and IP Source Guard, should be configured prior to configuration of QoS policies to avoid the potential conflict in filter precedence order which can result when the binary configuration file is reloaded. In some rare cases, when QoS precedence's are configured before non- QoS applications that use filters—for example: UDP Forwarding and IP Source Guard—the QoS information saved in the binary configuration file may not be correctly reloaded to the switch. The greater the number of filter-using non-QoS applications per port, the greater the probability that the QoS information in the binary configuration file may be reloaded incorrectly. If the QoS information in the binary configuration file is reloaded incorrectly, some of the QoS precedence's may not be configured correctly.
Q02088900	**QoS, information**: The system performs bandwidth allocation for queues according to Strict Priority and WRR algorithm. When you configure shapers on queues with minimum rate, the system first queues traffic to ensure the minimum rate is achieved for all queues. The system then allocates the remaining egress bandwidth according to Strict Priority, WRR and shape maximum rate configured

Table continues…

Reference number	Description
	for each queue. In case the sum of shape minimum rates configured (queue shapers) exceeds the line rate, the minimum shape rate is assured for queue 1 and then the remaining bandwidth is distributed amongst the rest of the queues. The system uses the WRR algorithm to best assure that the minimum rates for the rest of the queues are achieved. Note: If you have ERS 4000 and ERS 5600, in the same scenario the ERS 5600 operates differently, depending on the active queue set, and may use strict priority, WRR and RR algorithms.
wi00860958	**RADIUS Accounting**: If RADIUS accounting is enabled and the switch/stack is reset, then the accounting messages sent to the RADIUS server will only include a `RADIUS Accounting Off` message (no `RADIUS Accounting Stop` messages will be sent for authenticated clients).
wi00878635	**RADIUS, EAP Server, NEAP Server, Fail Open VLAN**: While servers are unreachable and ports are in Fail_Open VLAN deletion of all of the RADIUS servers of a given type (e.g. all EAP Servers, all NEAP Servers) may result in clients not being properly re-authenticated or assigned to the appropriate RADIUS VLAN. **Workaround**: Do not delete all RADIUS server types when RADIUS servers are unreachable. Alternatively after the RADIUS servers are again reachable, manually clear the MAC address table on the EAP enabled ports using the interface configuration command **`clear mac-address-table interface fastEthernet <portlist>`**.
wi00864589	**RADIUS, Interim Updates**: After RADIUS accounting is disabled for a RADIUS server, interim updates will still be sent to that server, if they were previously enabled. It is recommended that you turn off interim updates also, if it is desired not to receive them.
wi00490762, wi00483513	**RSTP**: When operating as an RSTP root bridge and the Base Unit in a stack is reset, or the stack transitions to standalone mode, the system may not always generate the SNMP trap message indicating a change in RSTP root. **Workaround**: A local log message for nnRstNewRoot is always generated.
wi00484096	**show running-config**: When you execute the **`show running-config`** or **`show running-config module`** commands the system may take a longer time than expected to display the output. In systems with very large and complex configurations of 8 units in a stack it can take up to 4 minutes to complete the display of the command. This is considered normal behavior
wi00496736	**SNMPv3, ACG**: SNMPv3 user commands (for example, snmp-server user) are commented in the text configuration file generated by the switch or stack if running the SSH version of the switch software. This happens because the associated passwords cannot be put in clear text in the generated configuration file. Please note that when the configuration is loaded the SNMPv3 users are not recreated.
wi00489857	**SONMP**: A change in the operation of the SONMP-based auto topology means that directly connected BayStack 450 switches report a physical auto topology change every 70 seconds to the Avaya ERS 4000 switch. You can ignore this auto topology change message where there is a direct connection from the Avaya ERS 4000 to a BayStack 450 switch.
wi00942683	**Spanning Tree**: When changing the STP mode from STPG to RSTP, or from MSTP to RSTP, the learning on the ports from groups other than group 1 will be

Table continues…

Reference number	Description
	set to disabled. **Workaround**: You will need to re-enable STP on other STP groups if so desired after re-configuration of the switch.
wi00862444	**TACACS+, Layer3**: In a layer 3 environment if the management VLAN is not operational (no link is up on that VLAN), the switch does not generate TACACS+ packets, therefore no authentication can be performed against the TACACS+ server. **Workaround**: Ensure that management VLAN is up.
wi00491296	**Telnet, ASCII Config** : If you configure a very short telnet timeout value and then you connect to the switch using telnet to execute the CLI command copy config, to save the ASCII configuration to USB or TFTP, the configuration file may be incomplete for large or complex stack configurations. **Workaround**: It is recommended to set the minimum telnet timeout value to 5 minutes.
wi00491518	**VLACP**: When you disable VLACP globally or on a per interface basis, the system forwards the following incorrect message to the syslog server: `Port X re-enabled by VLACP.`
wi00933290	**VRRP, Management VLAN**: If you create a VRRP interface on the management VLAN, the VRRP information will not be saved in the configuration file. This is operating as intended. **Workaround**: Avaya recommends that VRRP should not be configured on the Management VLAN of the switch/stack.
wi00863879	**VRRP**: VRRP may become unstable when multiple VRRP instances with Fast Advertisement are enabled. **Workaround**: If a large number of VRRP instances are to be configured, it is recommended that the minimum Fast Advertisement Interval (FAI) is set to no less than 600ms.
wi00484079	**SNMP Traps, Temporary Base Unit**: If you create new SNMP Trap notification filters while the stack is operating in Temporary Base Unit (TBU) mode (that is the Base Unit has failed) then the new filters are not saved and are lost upon stack reboot. **Workaround**: If the stack is operating in TBU mode, reset the stack and then create the required SNMP Trap notification filters.
wi00491450	**Port Mirroring, XrxYtx, XrxYtxOrYrxXtx**: If you use port 1 as a mirror port in XrxYtx or port mirroring modes, then broadcast or multicast traffic mirrored to the port is doubled on the monitor port. **Workaround**: Use another port on the switch as the mirrored port.
wi00490753	**EAP, Fail Open VLAN**: When a device is moved into or out of the Fail Open VLAN, there is no notification to the end client that the VLAN has been changed. **Workaround**: It is recommended that if Fail Open VLAN is used, you should set the DHCP lease time to a short period so that clients regularly refresh their IP address leases. Alternatively, if a client has been moved to the Fail Open VLAN, then issuing a DHCP release and renew on the client obtains a new IP address appropriate for the Fail Open VLAN.
wi00862943	**802.1AB Integration / VLAN Name TLV**: Avaya IP Phone does not use information from 802.1AB VLAN Name TLV to configure Voice VLAN. Other devices will correctly set the Voice VLAN if the VLAN name is set to voice.
wi00859649, wi00859648	**802.1AB Integration / File Server TLV**: The File Server IP Address which the IP Phone is using is not advertised by some Avaya IP Handsets (9630, 9620L, 9630G, 9640, 9620C) back to the switch. This can result in the switch displaying

Table continues…

Reference number	Description
	null information as the configured file server for these IP phones. **Workaround**: Information on fileserver use can be obtained from the phone or call server.
wi00857043	**802.1AB Integration / Avaya 1100**: Avaya 1100E IP Phones using firmware SIP1120e04.00.04.00 will not be recognized by the 802.1AB integration capabilities of the switch, as these phones use the manufacturer name in the TIA-Tx-TLV of "Avaya-01" which is different from the expected value of "Avaya". **Workaround**: Avaya 1100 IP Phones can be configured via alternative means such as DHCP.
wi00483355	New VLANs created are not learned when all dot1 TLVs are already enabled on ports.
wi00483930	**EAP**: When EAP performs authentication through TTLS, the first authentication between the supplicant and the switch may fail but subsequent authentications will succeed. **Workaround**: If authentication fails when using EAP-TTLS, do one of the following: • Wait 30 seconds for the client to re-authenticate successfully • Use an alternative EAP authentication mechanism for the client
wi00897383	**ERS 4800, Port Statistics** On ERS 4800 models the port statistics for ipInDiscards are not incremented.

IPv6 limitations

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

Table 11: IPv6 limitations

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

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 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

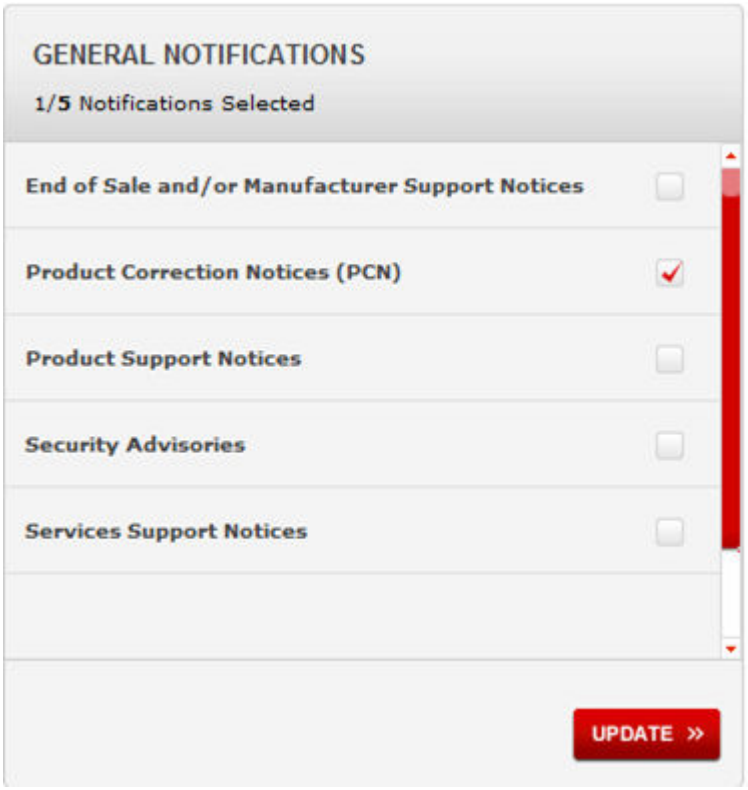
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

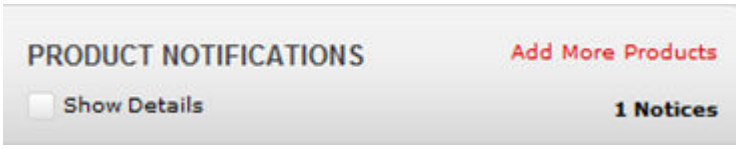
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services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

Procedure

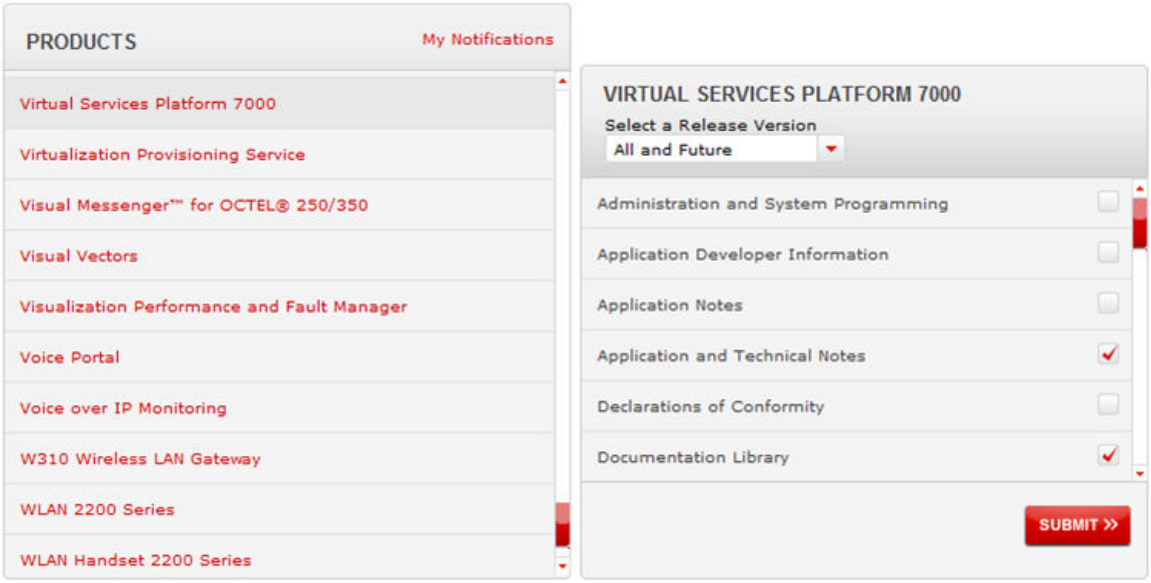
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click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



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



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.



11. Click **Submit**.