Release Notes for Avaya Ethernet Routing Switch 4900 and 5900 Series

Release 7.3
NN47211-400
Issue 05.04
December 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 and important information about the latest release. Release notes include a list of known issues (including workarounds where appropriate), known limitations and expected behaviors that may first appear to be issues.

This document describes new features, hardware, and known issues and limitations for the following products:

- Avaya Ethernet Routing Switch 4900 Series
- Avaya Ethernet Routing Switch 5900 Series

The information in this document supersedes applicable information in other documents in the suite.

Chapter 2: New in this release

The following sections detail what is new in *Release Notes for Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-400 for Release 7.3.

Ability to disable outbound SSH and Telnet clients

The purpose of this enhancement is to provide the ability to disable the ability to initiate outbound SSH and Telnet sessions from the switch. By default, outbound SSH and Telnet are available to users with Read-Only and Read-Write privileges.

The remote connection command is available to all users with Read-Write privileges. If desired to restrict which RW users can utilize the remote connection command, operate the switch in Enhanced Secure Mode utilizing Role Based Administration and limit access to the remote connection command. If enabled, all active outbound SSH and Telnet sessions are terminated immediately without warning.

The new ACLI command **`remote connection`** can be enabled and disabled using ACLI only. It is not supported through EDM or SNMP.

This enhancement is the result of GRIP 18201.

The following are the new ACLI commands:

- **`remote connection enable|disable`**
- **`show remote connection`**

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.

ECMP support for IP Shortcuts

The Equal Cost Multipath (ECMP) feature supports IP Shortcuts.

With ECMP, the switch can determine up to four equal-cost paths to the same destination prefix. You can use multiple paths for load sharing of traffic. These multiple paths allow faster convergence to other active paths in case of network failure. By maximizing load sharing among equal-cost paths,

you can use your links between routers more efficiently when sending IP traffic. Equal Cost Multipath is formed using routes from the same protocol.

For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series* and *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*.

New and modified ACLI commands

The following ACLI command is new:

- **`[no] [default] isis maximum-path <1–4>`**

The following ACLI command or output are modified:

- **`show ip route [isis]`**
- **`show ecmp`**

Fabric Attach enhancements

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

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

In Release 7.3, the FA feature provides the following enhancements:

Tagging mode on FA Client port updated based on client specific state

With Zero Touch auto-attach enabled, port VLAN tagging mode updates occur based on requirements signaled by discovered FA elements. Previously, tagging mode updates occurred based on I-SID/VLAN binding acceptance. When an FA element is deleted or has expired, all updated settings are cleared and rolled back to their previous values.

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.

Support Change of Authorization (COA) in FA Mode

This feature provides support for COA capabilities to reauthorize a client via EAPOL when the port is in Fabric Attach mode.

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.

Zero Touch Client

This feature provides basic Fabric Attach abilities for smaller installations where RADIUS implementations are not available or not justified.

Zero Touch Client (ZTC) functionality supports automatically updating port VLAN membership, the port PVID, and possibly the default port priority, based on the presence and type of discovered FA Clients. An I-SID/VLAN binding can be installed, as well.

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.

Trusted FA Client

The Trusted FA Client support allows I-SID/VLAN binding requests received from a FA Client to be selectively processed on secure ports (for example, ports under EAP/NEAP control). Previously, FA Client binding requests were ignored on secure ports.

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.

ACLI commands

FA enhancements introduce the following ACLI commands:

- **`fa zero-touch-client standard`**
- **`show fa zero-touch-client`**
- **`no fa-zero-touch-client`**
- **`default fa-zero-touch-client`**

EAP enhancements

The following EAP enhancements are available in this release:

ACLI command to verify RADIUS server reachability

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

This enhancement is the result of GRIP 16557.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.

RADIUS authentication fallback to secondary server

With this enhancement, each time a request to the primary RADIUS server times out after the expiration of all the configured retries, the switch queries the secondary RADIUS server as well.

This enhancement is the result of GRIP 16557.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.

Fail Open VLAN Recovery Improvement

When RADIUS server becomes reachable only those users that were not previously authenticated are authenticated.

This enhancement is the result of GRIP 16682.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.

RADIUS authentication delay

In scaled setups, there are two frequent problems when a burst of reauthentications occur:

1. RADIUS servers cannot respond to all of the requests
2. RADIUS servers can respond to all of the requests but the switch cannot process the requests

A delay time is introduced to delay RADIUS authentication when a burst is detected. RADIUS requests sent by the switch are limited to 50 per second and the reauthentication period for EAP and Non-EAP clients is reduced to a minimum of 60 seconds.

This enhancement is the result of GRIP 16682.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.

Track all MACs per port

The command **`show EAPOL sessions`** displays the authentication status of EAP and Non-EAP clients alongside with all unauthenticated clients connected to the switch or stack.

This command obsoletes **`show eapol multihost status`** and **`show eapol multihost non-eap-mac status`**.

This modification is the result of GRIP 16734.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.

RFC 4675 RADIUS attributes: Egress-VLANID and Egress-VLAN-NAME

This feature introduces support for two standard RADIUS attributes defined in RFC 4675: Egress-VLANID and Egress-VLAN-NAME. Using these attributes you can control the 802.1Q tagging for tragic egressing a port on a per VLAN basis where RADIUS authentication was performed for a connected EAP or non-EAP client.

This feature is the result of GRIP 17641.

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.

Delayed MAC authentication

The purpose of this feature is to give priority to EAP Authentication.

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

For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505 .

Support for FA bindings in CoA requests

This feature provides support for processing FA binding VSA attributes present in a CoA request.

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.

FA Client Dual-Key Authentication

With FA Client Dual Key Authentication, an FA Proxy or FA Server switch accepts either a factory default key or user defined key from FA client devices. When a user defined authentication key is configured on the FA Server or FA Proxy, the feature allows new unconfigured client devices to be authenticated with the default FA authentication key, without the need to configure the client device in order to connect to the network.

Use of the user defined key only or both the user defined key followed by the default key is controlled by user configuration (default setting utilizes both keys).

This EAP enhancement adds VSAs to support dual key authentication for FA Clients.

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.

Trusted FA Client

The Trusted FA Client support allows I-SID/VLAN binding requests received from a FA Client to be selectively processed on secure ports (for example, ports under EAP/NEAP control). Previously, FA Client binding requests were ignored on secure ports.

For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.

ACLI commands

The following new ACLI commands are supported:

- **`radius reachability check [eap | non-eap | global]`**
- **`eapol multihost radius-non-eap-delay [0–20]`**
- **`show eapol sessions`**

The following ACLI commands are obsolete:

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

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

PoE enhancements

You can configure a port to power up specific types of Powered Devices (PDs) using the **`poe poe-power-up-mode`** command. The default power up mode is 802.3at. For instance, the port mode can be configured as high inrush to supply power to a legacy PD that requires more than 15W at power-up.

The following ACLI command is new:

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

The following ACLI command outputs are modified:

- **show poe-port-status**
- **show running-config**

For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.

E-Tree and Private VLANs

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

- For more information about E-Tree, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series, NN47211-507*.
- For more information about Private VLANs, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series, NN47211-502*.

Overview of features and hardware models by release

This section provides an overview of which release introduced feature support for a particular platform. Each new release for a platform includes all the features from previous releases unless specifically stated otherwise.

Features for Releases

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

Features	Release by platform series	
	ERS 5900	ERS 4900
802.1AB (Link Layer Discovery Protocol) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB Avaya PoE Conservation Level Request TLV	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.		
802.1AB Avaya Call server TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB Avaya File server TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB Avaya 802.1Q Framing TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB Avaya Phone IP TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB customization For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB integration For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB (LLDP) MED Network Policy CLI For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB MED support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
802.1AB location TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
802.1AB new default parameters For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1D Compliancy Support For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
802.1X-2004 support For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1X non-EAP Accounting For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1X non-EAP re-authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1X or Non-EAP and Guest VLAN on same port For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1X or Non-EAP with Fail_Open VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1X or Non-EAP with VLAN name For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1X or Non-EAP use with Wake on LAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1X RFC3576 For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1x multiple host single authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.1x NEAP support (MAC authentication) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
802.3at LLDP based discovery For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Ability to manage device using IPv6 over SPB network For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.1	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
Ability to disable outbound SSH and Telnet clients For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.3	7.3
Ability to query USB file information For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.	7.2	7.2
Accounting Session ID enhancement For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.1	7.1
ACLI pipe filter commands For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.	7.2	7.2
ADAC (including 802.1ab support) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
ADAC and Auto QoS Interoperability	7.0	7.1
ADAC Uplink over SPBM For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
ASCII configuration file generator For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.	7.0	7.1
ASCII Download Enhancements For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
ASCII script config support	7.0	7.1
Automatic Unit Replacement For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501, *Logs Reference for Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000, 5900 Series and Virtual Services Platform 7000 Series*, NN47216-600 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
AUR enhancement	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.		
Automatic QoS and 802.1AB MED Interoperability For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
Autosave configuration enhancement For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Autotopology (802.1ab, SONMP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Boot/DHCP address assignment (RFC 1542)	7.0	7.1
Avaya Identity Engines Ignition Server For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Backup CONFIG file For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501, *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700 and *Logs Reference for Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000, 5900 Series and Virtual Services Platform 7000 Series*, NN47216-600.	7.0	7.1
boot partial-default command For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
BOOTP and DHCP RELAY For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Boot/DHCP address assignment (RFC 1542)	7.0	7.1
Booting with an ASCII configuration file from the local file system For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.1	7.1
BPDU filter For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
BPDU filtering on trunks For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.2	7.2
Broadcast rate limiting	7.0	7.1
Change RADIUS Password For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Circuitless IP For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Avaya Command Line Interface (CLI) For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.	7.0	7.1
CFM Integration with IP Shortcut For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.1	7.1
Circuit-less IPv6 (CLIP) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.1	7.1
CLI list command For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.	7.0	7.1
Configure asset ID For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Configurable route preference For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.2	7.2
CPU utilization For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503	7.0	7.1
Custom Autonegotiation Advertisement (CANA) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Default all EAP settings	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.		
Default IP For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
DHCP Client For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501, *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
DHCP Option 82 Support For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
DHCP Snooping For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
DHCP snooping external save For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Diagnostic Auto Unit Replacement (DAUR) enhancement For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.2	7.2
Distributed MultiLink Trunking (DMLT) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
Dual Syslog Server Support For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Dynamic ARP inspection For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
Dynamic Route Table Allocation For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
EAP enhancements: ACLI command to verify RADIUS server reachability, RADIUS authentication fallback to secondary server, Fail Open VLAN Recovery Improvement, RADIUS authentication delay, Track all MACs per port, RFC 4675 RADIUS attributes: Egress-VLANID and Egress-VLAN-NA, Delayed MAC authentication, Support for FA bindings in CoA requests, FA Client Dual-Key Authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505 and *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.3	7.3
EAP Fail Open with multi-VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
EAP and NEAP separation For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
EAP and non-EAP MultiVLAN capability For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
EAP-MD5 authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
EAPoL Multihost MAC-max For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
EAPoL (802.1x) MHSA/MHMV and Guest VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Energy Saver For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	7.0	7.1
Disable CLI audit log command For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Equal Cost MultiPath (ECMP) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
Equal Cost MultiPath (ECMP) support for IP Shortcuts For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506 and *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.3	7.3
Enhanced Secure Mode For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.2	7.2
Enterprise Device Manager For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.	7.0	7.1
EDM improved download support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
E-Tree For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.3	7.3
Extended IP Manager For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
Extended password history For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Fabric Attach For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.0	7.1
Fabric Attach updates: FA Server and FA Proxy functionality, FA Auto Provision For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.0.1	7.1
Fabric Attach updates: Tagging mode on FA Client port updated based on client specific state, Change of Authorization (COA) in FA Mode, Zero Touch Client, Trusted FA Client For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.3	7.3
Factory default command	7.0	7.1
Fail Open VLAN Continuity mode	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.		
Fail Open UBP For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.1	7.1
Show FLASH History For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Flow Control on gigabit Ethernet ports (802.3x) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Half duplex mode For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.2	7.2
Improved syslog capabilities For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Inactivity time out For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Increase Web-Server SSL key size	7.2	7.2
Independent VLAN Learning (IVL) support For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502 .	7.0	7.1
Internet Group Management Protocol version 2 (IGMPv2, RFC 2236) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Internet Group Management Protocol (IGMP) Querier For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Internet Group Management Protocol (IGMP v1/v2) Snooping and Proxy For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Internet Group Management Protocol (IGMP) version 3 For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.1	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
IP.CFG enhancements For more information, see *Installing Avaya Ethernet Routing Switch 5900 Series*, NN47211-300 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	7.0	7.1
IPFIX For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and*Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	7.0	7.1
IP local and static routes For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
IP Phone Automatic PoE Changes For more information, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-105.	7.0	7.1
IP Source Guard For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
IPv4 shortcuts For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.1	7.1
IPv6 over IPv4 Data Tunneling For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.1	7.1
IPv6 Automatic Address Assignment For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
IPv6 First Hop Security For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
IPv6 management For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
IPv6 static routes For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
IPv6 Source Guard For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.1	7.1
IPv6 tunneling For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Jumbo frames For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Layer 3 Brouter Port For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Layer 3 Virtual Router Redundancy Protocol For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Link Aggregation (802.3ad) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Link Layer Discovery Protocol (802.1AB) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Link-state tracking For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Lockout for failed logon attempts For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Logout CLI enhancement	7.0	7.1
Disable MAC Learning For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
MAC Flush For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
MAC security port lockout For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Many to Many Port Mirroring For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Multi-Link Trunking For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
MLT/DMLT/LAG Dynamic VLAN Changes For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
MLT and LAG Scaling For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
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 4900 and 5900 Series*, NN47211-502.	7.0	7.1
Multicast over SPB For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.0	7.1
Multicast Listener Discovery (MLD) snooping For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Multicast Listener Discovery Proxy For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.1	7.1
Multicast VLAN Registration For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.2	7.2
Multiple Hosts with Multiple VLANs for EAP-enabled ports (MHMV) auto configuration For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.1	7.1
Multiple local RW and RO user accounts	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.		
Multiple Spanning Tree groups (802.1s) **Note:** MSTP is the default spanning tree mode. For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
NEAP IP Phone support	7.0	7.1
NEAP not member of VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Network Time Protocol (NTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
New unit quick to config For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
NNI to NNI forwarding For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.2	7.2
Non-Local Static Routes For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Non local static routes for IPv6 For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.2	7.2
Non-unicast hashing over MLT/DMLT/LAG For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
Open Shortest Path First For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Out-of-band management	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Quick Start Configuration for Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-500.		
Password change via EDM For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Password complexity and password aging and lockout policy For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.2	7.2
Ping command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Ping Source Address For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
PoE enhancements: PoE high inrush mode For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.3	7.3
Port-based VLAN support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
Port mirroring (including ingress and egress) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Port operational status enhancements For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Port VLAN based mirroring For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.2	7.2
Private VLANs For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.3	7.3
Protocol-based VLAN support (including IPv6 protocol VLANs)	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.		
Protocol Independent Multicast-Sparse Mode (PIM-SM) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Protocol Independent Multicast-Source Specific Multicast (PIM-SSM) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.1	7.1
QoS - Diffserv Code Points (DSCP RFC2998) marking and classification For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
Quality of Service (QoS) - 802.1q For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
QoS Double Wide For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.1	7.1
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 4900 and 5900 Series*, NN47211-504.	7.0	7.1
Quality of Service (QoS) - Offset filtering (first 80 bytes) For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
QoS IP/L2 Filter Options For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
QoS Queue Set Support For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
QoS queue statistics For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
Quick start command and Web interface For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Remote Authentication Dial-In User Server (RADIUS)	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.		
RADIUS Accounting Enhancements (RFC2866) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
RADIUS Assigned VLAN update for 802.1x - use most recent RADIUS VLAN enhancement For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
RADIUS Server Reachability For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
RADIUS EAP or non-EAP requests from different servers For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
RADIUS Management Accounting with TACACS+ support For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
RADIUS Request use Management IP For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
RADIUS NEAP password configurable key For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
RADIUS attributes for EAP and NEAP authentications: Called- Station-Id and Calling-Station-Id For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0.1	7.1
Rapid Spanning Tree Protocol (802.1w) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
Reload command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Remote Monitoring (RMON)	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503		
Remote Switch Port ANalyzer For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Removal of partial-default requirement when enabling SPBM For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.2	7.2
Resilient stacking	7.0	7.1
RFC 3576 Disconnect and CoA support for NEAP clients For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505	7.1	7.1
Routing Information Protocol next generation (RIPng) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.2	7.2
RMON scaling For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
RO user access to telnet and SSH For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Routing Information Protocol For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
Routing Policies For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-506.	7.0	7.1
RSPAN over MLT/LACP For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.2	7.2
RSTP traps For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
RSTP SNMP traps For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.		
Run IP Office Script For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Run Scripts For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Running Configuration ACLI Display Commands For more information, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-105.	7.0	7.1
Scaling enhancements and corrections	7.1	7.1
Secure File Transfer Protocol (SFTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Secure Shell (SSH, SSHv2) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
sFlow For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.2	7
SFTP License and DHCP external support For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Show Environmental For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Show flash function For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
show ip netstat For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Show Port enhancement	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503 and *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.		
Show Software Status For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Show VLAN interface verbose command For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
Shutdown command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
SLAMon Agent For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
SLA Monitor For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
SLPP Guard For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
SLPP Guard on trunk For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.2	7.2
Simple Network Management Protocol (SNMP, SNMPv3) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Configurable SNMP trap port For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
SNMP Trap enhancements For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
SNMP traps for DHCP snooping/DAI/IPSG For more information, see *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
Simple Network Time Protocol (SNTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Software Licensing For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.	7.0	7.1
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 4900 and 5900 Series*, NN47211-502.	7.0	7.1
SPBM For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-507.	7.0	7.1
SSH banner For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
SSH Client For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
SSH RSA Authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
SSH retries For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Stack counters For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Stack monitor For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503 and *Logs Reference for Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000, 5900 Series and Virtual Services Platform 7000 Series*, NN47216-600.	7.0	7.1
Stack Forced Mode	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.		
Stack health check For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
Stack Health Monitoring and Recovery For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503.	7.0	7.1
Stack loopback tests For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1
Static FDB MAC Entry For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
Sticky MAC Address For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Storm control For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
STP BPDU filtering ignore-self For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
Syslog Support for 802.1X/EAP/NEAP/UBP For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
TACACS+ For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
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.	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
Terminal Mode Permanent Setting	7.0	7.1
Time Domain Reflectometer For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Trace Functions For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-503 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Trace Support for 802.1X For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Traffic Profile Filter Set Support For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504.	7.0	7.1
Trivial File Transfer Protocol (TFTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501.	7.0	7.1
Disable USB and console For more information, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
User Based Policies For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-504 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Username password enhancement For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.	7.0	7.1
Virtual LACP For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1
VLAN Scaling	7.0	7.1
Voice VLAN Integration For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502.	7.0	7.1

Table continues…

Features	Release by platform series	
	ERS 5900	ERS 4900
Web User Interface (http and https)	7.0	7.1
WebUI MIB Web Page	7.0	7.1
WebUI Trap Web Page	7.0	7.1
Write memory and save config command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104	7.0	7.1
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 4900 and 5900 Series*, NN47211-104 and *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505	7.0	7.1
Auto Detection Auto Configuration (ADAC) - modify the 802.1AB detection mechanism used in ADAC to work correctly with the Avaya IP handsets	7.0	7.1
Increase PoE power For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-501 and *Troubleshooting Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-700.	7.0	7.1

Hardware models

The following tables provides list of hardware models in ERS 5900 and ERS 4900 Series.

Table 1: Ethernet Routing Switch 5900 Series

Switch model	Part number	Description	Initial Release
ERS 59100GTS	AL5900A5x-E6	ERS 59100GTS with base software license, no fans, no PSU, no power cord	7.2
	AL5900x5B-E6	ERS 59100GTS with base software license, two fan tray modules, back to front 450 Watt PSU, power cord	7.2
	AL5900x5F-E6	ERS 59100GTS with base software license, two fan tray modules, front to back 450 Watt PSU, power cord	7.2
ERS 59100GTS-PWR+	AL5900A6x-E6	ERS 59100GTS-PWR+ with base software license, no fans, no PSU, no power cord	7.2
	AL5900x6B-E6	ERS 59100GTS-PWR+ with base software license, two fan tray modules, back to front 1400 Watt PSU, power cord	7.2

Table continues…

Switch model	Part number	Description	Initial Release
	AL5900x6F-E6	ERS 59100GTS-PWR+ with base software license, two fan tray modules, front to back 1400 Watt PSU, power cord	7.2
ERS 5928GTS-uPWR	AL590007X-E6	ERS 5928GTS-uPWR with base software license, no fans, no power supply unit (PSU), no power cord	7.1
	AL5900x7B-E6	ERS 5928GTS-uPWR with base software license, two fan tray modules, back to front 1400 Watt PSU, power cord	7.1
	AL5900x7F-E6	ERS 5928GTS-uPWR with base software license, two fan tray modules, front to back 1400 Watt PSU, power cord	7.1
ERS 5928GTS	AL590001X-E6	ERS 5928GTS with base software license, no fans, no power supply unit (PSU), no power cord	7.0
	AL5900x1B-E6	ERS 5928GTS with base software license, two fan tray modules, back to front 450 Watt PSU, power cord	7.0
	AL5900x1F-E6	ERS 5928GTS with base software license, two fan tray modules, front to back 450 Watt PSU, power cord	7.0
ERS 5928GTS-PWR+	AL590002X-E6	ERS 5928GTS-PWR+ with base software license, no fans, no PSU, no power cord	7.0
	AL5900x2B-E6	ERS 5928GTS-PWR+ with base software license, two fan tray modules, back to front 1400 Watt PSU, power cord	7.0
	AL5900x2F-E6	ERS 5928GTS-PWR+ with base software license, two fan tray modules, front to back 1400 Watt PSU, power cord	7.0
ERS 5952GTS	AL590003X-E6	ERS 5952GTS with base software license, no fans, no PSU, no power cord	7.0
	AL5900x3B-E6	ERS 5952GTS with base software license, two fan tray modules, back to front 450 Watt PSU, power cord	7.0
	AL5900x3F-E6	ERS 5952GTS with base software license, two fan tray modules, front to back 450 Watt PSU, power cord	7.0
ERS 5952GTS-PWR+	AL590004X-E6	ERS 5952GTS-PWR+ with base software license, no fans, no PSU, no power cord	7.0
	AL5900x4B-E6	ERS 5952GTS-PWR+ with base software license, two fan tray modules, back to front 1400 Watt PSU, power cord	7.0

Table continues…

Switch model	Part number	Description	Initial Release
	AL5900x4F-E6	ERS 5952GTS-PWR+ with base software license, two fan tray modules, front to back 1400 Watt PSU, power cord	7.0
*__Note__: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.			

For more information about ERS 5900 Series, see *Installing Avaya Ethernet Routing Switch 5900 Series*, NN47211-300.

Table 2: Ethernet Routing Switch 4900 Series

Switch model	Part number	Description	Initial Release
ERS4926GTS	AL4900x01-E6 **Note:** Replace the “x” with a country specific power cord code. See the footnote for details.	ERS 4926GTS with base software license, one 250 Watt PSU, .5 M stack cable, power cord	7.1
ERS 4926GTS-PWR+	AL4900x02-E6 **Note:** Replace the “x” with a country specific power cord code. See the footnote for details.	ERS 4926GTS-PWR+ with base software license, one 250 Watt PSU, .5 M stack cable, power cord	7.1
ERS 4950GTS	AL4900x03-E61 **Note:** Replace the “x” with a country specific power cord code. See the footnote for details.	ERS 4950GTS with base software license, one 1025 Watt PSU, .5 M stack cable, power cord	7.1

Table continues…

Switch model	Part number	Description	Initial Release
ERS 4950GTS-PWR+	AL4900x04-E6 **Note:** Replace the “x” with a country specific power cord code. See the footnote for details.	ERS 4950GTS-PWR+ with base software license, one 1025 Watt PSU, .5 M stack cable, power cord	7.1
*__Note__: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.			

For more information about ERS 4900 Series, see *Installing Avaya Ethernet Routing Switch 4900 Series*.

Chapter 3: Important notices and new features

This section describes important software and hardware related notices.

The warranty includes access to software updates for features and maintenance releases.

Release file names

This section lists the software files for the following platforms:

- Ethernet Routing Switch 4900 Series
- Ethernet Routing Switch 5900 Series

Table 3: Software components

File Type	ERS 4900 Series		ERS 5900 Series	
	File Name	File Size (bytes)	File Name	File Size (bytes)
Secure runtime image	4900_730007s.img	17,598,564	5900_730007s.img	17,770,612
Diagnostic software version	5900_72005_diags.bin	6,409,424	5900_72005_diags.bin	6,409,424
Enterprise Device Manager Help Files	ers5000v730_HELP_EDM.zip	1,942,219	ers5000v730_HELP_EDM.zip	1,942,219
MIB Definition File Archive	Ethernet_Routing_Switch_4900_MIBs_7.3.0.zip	1,548,172	Ethernet_Routing_Switch_5900_MIBs_7.3.0.zip	1,661,409
EDM Plug in	ers5900v7.3.0.0.zip	3,488,570	ers5900v7.3.0.0.zip	3,488,570

Software upgrade

This section provides procedures to upgrade the software — diagnostic and agent software.

Note:

VLAN ID 4060 is used internally by SPBM with IP Shortcuts Multicast and cannot be created on ERS 5900 and ERS 4900.

Before upgrading, if VLAN ID 4060 exists, then migrate it to a different VLAN ID.

Upgrade considerations for Enhanced Secure Mode

Upgrading from a previous version not supporting Enhanced Secure Mode maintains the existing non Enhanced Secure configuration. If you switch to Enhanced Secure Mode after upgrade, the configuration is defaulted.

Upgrading to a newer release supporting Enhanced Secure Mode maintains the existing configuration parameters including the following:

- Users and passwords
- Network configuration
- Settings for TFTP, TELNET, SSH protocols

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

Upgrading diagnostic software

Use the following procedure for upgrading the diagnostic software image.

1. Access the ACLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the **`enable`** command.
3. Use the command **`download address [usb] <ip_address> diag <image_name> [no reset]`** to transfer the diagnostic image to the device.

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

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the diagnostic image is hosted.
diag <image_name>	The name of the diagnostic image file on the TFTP server.
no-reset	This parameter specifies that the device will not reset after the upgrade is complete.
usb	This parameter specifies that the software download will occur from a USB device instead of the network.

The upgrade process 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 process.

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

During the download process the switch is not operational.

Upgrading agent software

Use this procedure to upgrade agent software.

1. Access the ACLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the **enable** command.
3. Use the command **download address [usb] <ip_address> {primary | secondary} {image <image_name> | image-if-newer <image_name> | poe_module_image <image_name>} [no-reset]** to transfer the agent image to the device.

The following table describes the parameters for this command.

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the agent image is hosted.
primary | secondary	Designates whether the image is stored in the primary or secondary image location. The default is primary.
image <image_name> | image-if-newer <image_name> | poe_module_image <image_name>	The name of the agent image file on the TFTP server. Each option is mutually exclusive. Use the option described with the following situation: • To load the agent image under normal circumstances, use the image option. • To load the agent image only if it is newer than the current image, use the image-if-newer option. • To load the agent image if it is a PoE module image, use the poe_module_image option.
no-reset	Specifies that the device will not reset after the upgrade is complete.
usb	Specifies that the software download will occur from a USB device instead of the network.

The upgrade process 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 process.

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

During the download process the switch is not operational.

Using TLS1.2 certificate and resetting SSL server

About this task

The RSA key size is increased from 1024 bit to 2048 bit in Release 7.2. After upgrading, use the following procedure to use TLS 1.2 certificate and reset the SSL server.

Note:

If you are upgrading from Release 7.2, you do not need to perform this procedure again.

Procedure

1. Enter the following command to replace the SSL certificate:

   ```
   ssl certificate
   ```

2. Enter `y` to create the certificate.
3. Enter the following command to reset the SSL server:

   ```
   ssl reset
   ```

Example

```
Switch(config)#ssl certificate
Certificate already exists. Create it anyway (y/n) ? y
Switch(config)#ssl reset
```

How to get EDM online help files for embedded EDM

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

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

For more information about EDM, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.

Downloading help files

Before you begin

- An available TFTP server

About this task

Use this procedure to download EDM online help files.

Procedure

1. To obtain EDM help files for the embedded element manager, do one of the following:
   - Go to the Avaya Web site at http://www.avaya.com/support and locate the help files for the appropriate product.
   - Select the help files from the software CD ROM.
2. Download the help files to a TFTP server.

How to configure the path to the embedded EDM help files

If you are using embedded EDM, use the procedures in this section to configure the path to the help files. You can configure the help file path with ACLI or EDM.

Configuring the path to the help files using ACLI

About this task

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

Procedure

In ACLI, go to the Global Configuration mode and use the following command:

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

The following table describes the parameters for the edm-help-file-path command.

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

Example

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

```
edm help-file-path ERS5900_xx_Help tftp address 100.100.100.15
```

In the preceding example, xx is the software release version and ERS5900_xx_Help is a folder that contains help files. The folder is located on a TFTP server at the 100.100.100.15 address.

Configuring the path to the help files using EDM

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

Procedure steps

1. From the navigation tree, click **Edit**.
2. From the Edit tree, click **File System**.
3. Select the **Help File Path** tab.
4. In the Path dialog box, enter the path to the help file storage location.

   Example

   tftp://xxx.xxx.xxx.xxx/file_name

Tested browsers

EDM has been tested with the following web browsers:

- Microsoft Internet Explorer 11.0
- Mozilla Firefox 45.0.2

Supported software and hardware capabilities

This section lists software scaling capabilities of the following products:

- Ethernet Routing Switch 4900 Series
- Ethernet Routing Switch 5900 Series

Table 4: Supported software and hardware scaling capabilities

Unless stated otherwise, the capabilities are listed per stack, where a stack consists of one to eight units.

Feature	ERS 5900 Series	ERS 4900 Series
SPB:		
SPB nodes for each region	1000	750

Table continues…

Feature	ERS 5900 Series	ERS 4900 Series
IS-IS adjacencies	4	4
BEBs for each region	512[1]	512[1]
CVLANs	1000	500
SPB Switched UNI	500	500
SPB ISIDs (Maximum L2 VSN)	1000	500
Maximum Multicast Streams	512	512
Max L2 VSN with Multicast enabled	256	256
Operational modes	Standalone or stacked 8 high [2]	Standalone or stacked 8 high
B-VLANs	2	2
IS-IS interfaces	4	4
IPv6:		
Maximum IPv6 in IPv4 data tunnels	16	16
IPv6 DHCP relay forwarding paths for each unit or stack	256	256
IPv6 Static Routes	512	512
IPv6 interfaces	256	256
IPv6 Routes total (includes learned routes, static and local routes	2048	2048
IPv6 Dynamic routing interfaces	64	64
QoS:		
Per port egress queues	8	8
QoS precedence for each ASIC	16	16
QoS rules for each precedence	256	256
Total QoS rules	4096	4096
Performance:		
MAC address capacity	32768	32768
Stacking port bandwidth, FDX	42 Gbps	26 Gbps
Maximum ports for each stack	416	416
Miscellaneous:		
Maximum port mirroring instances	4	4
Maximum admin accounts	10	10
RSPAN VLANs	4	4
RSPAN destinations for each unit or stack	4	4

Table continues…

Feature	ERS 5900 Series	ERS 4900 Series
802.1X (EAP) clients for each port, MHMV	32	32
802.1X (EAP) clients for each MHSA	1 authenticated / balance unlimited	1 authenticated / balance unlimited
802.1x (EAP and NEAP) clients for each switch or stack	768	768
Maximum RADIUS servers	2	2
Maximum 802.1X EAP servers	2	2
Maximum 802.1X NEAP servers	2	2
Maximum RADIUS/EAP/NEAP servers	6	6
IPFix number of sampled flows	100000	100000
RMON alarms	800	800
RMON events	800	800
RMON Ethernet history	249	249
RMON Ethernet statistics	110	110
Link State Tracking instances	2	2
sFlow maximum number of collectors	4	4
sFlow minimum packet sampling rate	1 out of 4096	1 out of 4096
Layer 2:		
Concurrent VLANs	1024	1024
Supported VLAN IDs	1 – 4094 (0 and 4095 reserved. 4001 reserved by STP. 4002-4008 reserved by multiple STP)	1 – 4094 (0 and 4095 reserved. 4001 reserved by STP. 4002-4008 reserved by multiple STP)
	Note: VLAN ID 4060 cannot be created on ERS 5900 and ERS 4900. Before upgrading ERS 5900 from Release 7.0 to later release, if VLAN ID 4060 exists, then migrate it to a different VLAN ID.	
Protocol VLAN types	16	16
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32	32
Links or ports for MLT, DMLT or LAG	8	8
Static MAC addresses	1024	1024

Table continues…

Feature	ERS 5900 Series	ERS 4900 Series
Spanning Tree Group instances (802.1s)	8	8
Avaya Spanning Tree Groups	8	8
DHCP Snooping table entries for each unit	1024	1024
LLDP Neighbors for each port	16	16
LLDP Neighbors for each switch or stack	800	800
Private VLANs	200	200
Layer 3:		
IP Interfaces (VLANs or Brouter ports)	256	256
ARP Entries total (local, static and dynamic)	4096	1792
ARP Entries — local (IP interfaces for each switch or stack)	256	256
ARP Entries — static	256	256
ARP Entries — dynamic	3584	1280
IPv4 Routes total (local, static and dynamic)	4096	2048
IPv4 Static routes	512	512
IPv4 Local routes	256	256
IPv4 Dynamic routes (RIP and OSPF)	4096	2048
Dynamic Routing interfaces (RIP and OSPF)	64	64
OSPF areas	4	4
OSPF adjacencies (devices for each OSPF areas)	32	32
OSPF Link State Advertisements (LSA)	10000	10000
OSPF virtual links	4	4
OSPF host routes	32	32
ECMP (Maximum concurrent equal cost paths)	4	4
ECMP (Max next hop entries)	256	128
VRRP instances	256	256
Management routes	4	4
UDP forwarding entries	128	128

Table continues…

Feature	ERS 5900 Series	ERS 4900 Series
DHCP relay entries	256	256
DHCP relay forward paths	512	512
Multicast:		
IGMP v1, v2 and v3 multicast groups	1024	1024
IGMP enabled VLANs	256	256
MLD snooping enabled VLANs	512 MLDv1 entries 256 MLDv2 entries	512 MLDv1 entries 256 MLDv2 entries
PIM-SM forward entries for each stack	1024	512
PIM-SM interfaces (active and passive)	64 (4 active and 60 passive)	32 (4 active and 28 passive)

[1] Maximum number of BEBs for each region can be reduced when SPB Multicast is enabled or when connecting to IST switches.

[2] ERS 59100GTSand ERS 59100GTS-PWR+ support only four units high stack.

Licensing support

Avaya Product Licensing and Delivery System (PLDS) provides self-service license activations, upgrades and moves/changes.

You must obtain appropriate license for the following features:

- Open Shortest Path First (OSPF)
- Virtual Router Redundancy Protocol (VRRP)
- Equal Cost Multi Path (ECMP)
- Protocol Independent Multicast-Sparse mode (PIM-SM)
- IPv6 Forwarding
- IP Shortcuts
- Routing Information Protocol next generation (RIPng)

All other features in Release 7.3 are included with the base license.

You can obtain a trial license to try out advanced license features for 60 days. Trial licenses are available from Avaya at no charge. Trial licenses need to be ordered from Avaya and can be obtained using the PLDS license delivery system. After the trial period expires, the licensed feature is disabled.

The PLDS Advanced trial license is generated using the system MAC address of a switch and can only be generated and used once for a given MAC address. After the expiry of the 60 day trial period, you will see messages on the console and in the alarms database that the license has

expired. If you restart the system after the license expiration, the Advanced features will not be loaded even if they are in the saved configuration. If you purchase an Advanced license, you must obtain and install a license file. For more information about how to generate a license file, see *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300.

For more information about PLDS and installing a license file, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-104.

Supported standards, MIBs, and RFCs

This section lists the supported standards, MIBs, and RFCs.

Standards

The following IEEE Standards contain information that applies to this switch:

IEEE 802.1D	Spanning Tree Protocol
IEEE 802.1w	Rapid Spanning Tree
IEEE 802.1s	Multiple Spanning Tree
IEEE 802.1t 802.1D	Maintenance
IEEE 802.1p	Prioritizing
IEEE 802.1Q	VLAN Tagging
IEEE 802.1X	Ethernet Authentication Protocol
IEEE 802.1AB	Link Layer Discovery Protocol
IEEE 802.1AX	Link Aggregation Control Protocol (LACP)
IEEE 802.1ag	Connectivity and Fault Management
IEEE 802.1aq	Shortest Path Bridging MAC
IEEE 802.3	Ethernet
IEEE 802.3af	Power over Ethernet
IEEE 802.3at	Power over Ethernet Plus
IEEE 802.3ad / 802.1AX	Link Aggregation Control Protocol
IEEE 802.3ab	Gigabit Ethernet over Copper
IEEE 802.3ae	10 Gbps Ethernet
IEEE 802.3ak	10GBase-CX4
IEEE 802.3i	10Base-T
IEEE 802.3u	Fast Ethernet
IEEE 802.3x	Flow Control
IEEE 802.3z	Gigabit Ethernet

RFCs

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

Table 5: Supported RFCs

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 768 UDP	7.0	7.1
RFC 783 TFTP	7.0	7.1
RFC 792 ICMP	7.0	7.1
RFC 793 TCP	7.0	7.1
RFC 826 ARP	7.0	7.1
RFC 854 Telnet	7.0	7.1
RFC 894 IP over Ethernet	7.0	7.1
RFC 903 Reverse ARP	7.0	7.1
RFC 950 / RFC 791 IP	7.0	7.1
RFC 951 BootP	7.0	7.1
RFC 1058 RIPv1	7.0	7.1
RFC 1112 IGMPv1	7.0	7.1
RFC 1122 Requirements for Internet hosts	7.0	7.1
RFC 1155 SMI	7.0	7.1
RFC 1156 MIB for management of TCP/IP	7.0	7.1
RFC 1157 SNMP	7.0	7.1
RFC 1212 Concise MIB definitions	7.0	7.1
RFC 1213 MIB-II	7.0	7.1
RFC 1215 SNMP Traps Definition	7.0	7.1
RFC 1305 NTP version3	7.0	7.1
RFC 1340 Assigned Numbers	7.0	7.1
RFC 1350 TFTP	7.0	7.1
RFC 1354 IP Forwarding Table MIB	7.0	7.1
RFC 1398 Ethernet MIB	7.0	7.1
RFC 1442 SMI for SNMPv2	7.0	7.1
RFC 1450 MIB for SNMPv2	7.0	7.1
RFC 1493 Bridge MIB	7.0	7.1
RFC 1591 DNS Client	7.0	7.1

Table continues…

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 1650 Definitions of Managed Objects for Ethernet-like Interfaces	7.0	7.1
RFC 1724 / RFC 1389 RIPv2 MIB extensions	7.0	7.1
RFC 1769 / RFC 1361 SNTP	7.0	7.1
RFC 1886 DNS extensions to support IPv6	7.0	7.1
RFC 1908 Coexistence between SNMPv1 & v2	7.0	7.1
RFC 1945 HTTP v1.0	7.0	7.1
RFC 1981 Path MTU Discovery for IPv6	7.0	7.1
RFC 2011 SNMP v2 MIB for IP	7.0	7.1
RFC 2012 SNMP v2 MIB for TDP	7.0	7.1
RFC 2013 SNMP v2 MIB for UDP	7.0	7.1
RFC 2080 Routing Information Protocol next generation (RIPng)	7.2	7.2
RFC 2096 IP Forwarding Table MIB	7.0	7.1
RFC 2131 / RFC 1541 Dynamic Host Configuration Protocol (DHCP)	7.0	7.1
RFC 2138 RADIUS Authentication	7.0	7.1
RFC 2139 RADIUS Accounting	7.0	7.1
RFC 2236 IGMPv2	7.0	7.1
RFC 2328 / RFC 2178 / RFC 1583 OSPFv2	7.0	7.1
RFC 2453 RIPv2	7.0	7.1
RFC 2454 IPv6 UDP MIB	7.0	7.1
RFC 2460 IPv6 Specification	7.0	7.1
RFC 2461 IPv6 Neighbor Discovery	7.0	7.1
RFC 2464 Transmission of IPv6 packets over Ethernet	7.0	7.1
RFC 2474 Differentiated Services (DiffServ)	7.0	7.1
RFC 2541 Secure Shell protocol architecture	7.0	7.1
RFC 2597 Assured Forwarding PHB Group	7.0	7.1
RFC 2598 Expedited Forwarding PHB Group	7.0	7.1
RFC 2616 / RFC 2068 HTTP 1.1	7.0	7.1
RFC 2660 HTTPS - Secure Web	7.0	7.1
RFC 2665 / RFC 1643 Ethernet MIB	7.0	7.1
RFC 2674 Q-BRIDGE-MIB	7.0	7.1
RFC 2710 Multicast Listener Discovery version 1 (MLDv1)	7.0	7.1
RFC 2715 Interoperability Rules for Multicast Routing Protocols	7.0	7.1
RFC 2787 Definitions of Managed Objects for VRRP	7.0	7.1

Table continues…

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 2819 / RFC 1757 / RFC 1271 RMON	7.0	7.1
RFC 2851 Textual Conventions for Internet network addresses	7.0	7.1
RFC 2863 / RFC 2233 / RFC 1573 Interfaces Group MIB	7.0	7.1
RFC 2865 RADIUS	7.0	7.1
RFC 2866 / RFC 2138 RADIUS Accounting	7.0	7.1
RFC 2869 RADIUS Extensions - Interim updates	7.0	7.1
RFC 2933 IGMP MIB	7.0	7.1
RFC 3058 RADIUS Authentication	7.0	7.1
RFC 3140 / RFC 2836 Per-Hop Behavior Identification codes	7.0	7.1
RFC 3162 RADIUS and IPv6	7.0	7.1
RFC 3195 Reliable delivery Syslog (only in Enhanced Secure Mode)	7.2	7.2
RFC 3246 Expedited Forwarding Per-Hop Behavior	7.0	7.1
RFC 3260 / RFC 2475 Architecture for Differentiated Services	7.0	7.1
RFC 3289 DiffServ MIBs	7.0	7.1
RFC 3315 DHCPv6	7.0	7.1
RFC 3410 / RFC 2570 SNMPv3	7.0	7.1
RFC 3411 / RFC 2571 SNMP Frameworks	7.0	7.1
RFC 3412 / RFC 2572 SNMP Message Processing	7.0	7.1
RFC 3413 / RFC 2573 SNMPv3 Applications	7.0	7.1
RFC 3414 / RFC 2574 SNMPv3 USM	7.0	7.1
RFC 3415 / RFC 2575 SNMPv3 VACM	7.0	7.1
RFC 3416 / RFC 1905 SNMP	7.0	7.1
RFC 3417 / RFC 1906 SNMP Transport Mappings	7.0	7.1
RFC 3418 / RFC 1907 SNMPv2 MIB	7.0	7.1
RFC 3484 Default Address Selection for IPv6	7.0	7.1
RFC 3513 IPv6 Addressing Architecture	7.0	7.1
RFC 3569 Overview of Source Specific Multicast (SSM)	7.0	7.1
RFC 3579 RADIUS support for EAP	7.0	7.1
RFC 3584 / RFC 2576 Co-existence of SNMP v1/v2/v3	7.0	7.1
RFC 3587 IPv6 Global Unicast Format	7.0	7.1
RFC 3596 DNS extensions to support IPv6	7.0	7.1
RFC 3621 Power over Ethernet MIB	7.0	7.1
RFC 3635 Definitions of Managed Objects for the Ethernet-like Interface Types	7.0	7.1

Table continues…

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 3768 / RFC 2338 VRRP	7.0	7.1
RFC 3810 MLDv2 for IPv6	7.0	7.1
RFC 3826 AES for the SNMP User-based Security Model	7.0	7.1
RFC 3917 Requirements for IPFIX	7.0	7.1
RFC 3954 Netflow Services Export v9	7.0	7.1
RFC 3993 DHCP Subscriber-ID sub-option	7.0	7.1
RFC 4007 Scoped Address Architecture	7.0	7.1
RFC 4022 / RFC 2452 TCP MIB	7.0	7.1
RFC 4113 UDP MIB	7.0	7.1
RFC 4133 / RFC 2737 / RFC 2037 Entity MIB	7.0	7.1
RFC 4193 Unique Local IPv6 Unicast Addresses	7.0	7.1
RFC 4213 Transition Mechanisms for IPv6 Hosts & Routers	7.0	7.1
RFC 4250 SSH Protocol Assigned Numbers	7.0	7.1
RFC 4251 SSH Protocol Architecture	7.0	7.1
RFC 4252 SSH Authentication Protocol	7.0	7.1
RFC 4253 SSH Transport Layer Protocol	7.0	7.1
RFC 4254 SSH Connection Protocol	7.0	7.1
RFC 4291 IPv6 Addressing Architecture	7.0	7.1
RFC 4293 IPv6 MIB	7.0	7.1
RFC 4344 SSH Transport layer Encryption Modes	7.0	7.1
RFC 4345 Improved Arcfour Modes for SSH	7.0	7.1
RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6	7.0	7.1
RFC 4432 SSHv2 RSA	7.0	7.1
RFC 4443 / RFC 2463 ICMPv6 for IPv6	7.0	7.1
RFC 4541 Considerations for IGMP and MLD snooping switches	7.0	7.1
RFC 4601 Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification	7.0	7.1
RFC 4604 / RFC 3376 IGMPv3	7.0	7.1
RFC 4632 Classless Inter-domain Routing (CIDR)	7.1	7.1
RFC 4673 RADIUS Dynamic Authorization Server MIB	7.0	7.1
RFC 4675 Egress-VLAN-Name and Egress-VLANID attributes (partial support)	7.3	7.3
RFC 4716 SSH Public Key File Format	7.0	7.1
RFC 4750 / RFC 1850 / RFC 1253 OSPF v2 MIB	7.0	7.1
RFC 4789 SNMP over IEEE 802 Networks	7.0	7.1

Table continues…

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 4861 Neighbor Discovery for IPv6	7.0	7.1
RFC 4862 / RFC 2462 IPv6 Stateless Address Auto-Configuration	7.0	7.1
RFC 5010 / RFC 3046 DHCP Relay Agent Information Option 82	7.0	7.1
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6	7.0	7.1
RFC 5101 Specification of the IP Flow Information Export (IPFIX) Protocol for Exchange of IP Traffic	7.0	7.1
RFC 5176 / RFC 3576 Dynamic Authorization Extensions to RADIUS	7.0	7.1
RFC 5186 IGMPv3/MLDv2 and Multicast Routing Interaction	7.0	7.1
RFC 5246 TLS Protocol Version 1.2	7.1	7.1
RFC 6329 IS-IS Extensions Supporting Shortest Path Bridging	7.0	7.1

Table 6: Obsolete RFCs

RFC	Obsolete Release
RFC 1519 Classless Inter-Domain Routing (CIDR)	7.1

The following table lists IPv6 specific RFCs.

Table 7: IPv6 specific RFCs

Standard	Description	Compliance
RFC 1886	DNS Extensions to support IPv6	Supported
RFC 1981	Path MTU Discovery for IPv6	Supported
RFC 2080	Routing Information Protocol next generation (RIPng)	Supported
RFC 2460	Internet Protocol v6 (IPv6) Specification	Supported
RFC 2461	Neighbor Discovery for IPv6	Supported
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 3162	RADIUS and IPv6	Supported
RFC 3315	DHCPv6	Support for IPv6 DHCP Relay
RFC 3587	IPv6 Global Unicast Format	Supported
RFC 3596	DNS extensions to support IPv6	Supported
RFC 3810	MLDv2 for IPv6	Supported
RFC 4007	Scoped Address Architecture	Supported

Table continues…

Standard	Description	Compliance
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack and configured tunnels
RFC 4291	IPv6 Addressing Architecture	Support earlier version of RFC (3513)
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4429	Optimistic Duplicate Address Detection (DAD) for IPv6	Supported
RFC 4443	Internet Control Message Protocol (ICMPv6)	Support earlier version of RFC (2463)
RFC 4541	Considerations for IGMP and MLD snooping switches	Supported
RFC 4861	Neighbor Discovery for IPv6	Supported
RFC 4862 / RFC 2462	IPv6 Stateless Address Auto-Configuration	Supported
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6	Supported

Chapter 4: Resolved issues

The following table lists the issues resolved in this software release.

Table 8: Issues resolved in Release 7.3

Change Request number	Description
ERS495900-829	SPBM Multicast scaling: Bouncing redundant links causes stack to be unstable and traffic loss. It recovers after 15 minutes.
ERS495900-2188	Traffic does not recover when MLT ports that form NNI are shut down.
ERS495900-13	FOV Continuity Mode: NEAP clients are removed from NEAP authenticated list after standalone to stack transition.
ERS495900-2791	Syslog messages with severity level 3 (Critical) are not sent to the remote syslog server
ERS495900-2700	ERS 5952 PoE+ - Camera not getting enough power without LLDP - Power is given up to 15W camera requires 25.5
ERS495900-3026	After enabling SNTP server, Msgtime field vlaue on EDM changes to a unknown value
ERS495900-3034	ERS 4900 upgraded to 7.2.0.009 after which access to the switch is denied by radius server. Issue is random and click after 2-3 weeks.
ERS495900-3056	ERS4926GTS-PWR+: download image file via tftp causing uplink SFP+ port flap using SFP gbic
ERS495900-3294	ERS 4900 v7.2.0 Client do not communicate with EAP and SPB when fail-open-vlan is configured
wi01207480/ ERS495900-87	After the password aging time expires, the user cannot change the password using EDM and connect to EDM.
wi01198235/ ERS495900-57	The L2 TraceMroute tab in EDM is empty.
wi01209636/ ERS495900-95	SPBM Multicast: Multicast stream is not removed when access ports are disabled. Multicast streams will be aged out.
wi01219325/ ERS495900-134	The information displayed in the Interface SPBM tab in EDM is doubled. The ACLI command works as expected.
wi01222045/ ERS495900-162	Telnet session is disconnected when IP routing is disabled from an EDM console session.

Table continues…

Change Request number	Description
wi01222711/ ERS495900-178	MHMV clients are lost after transitioning from stack to standalone or standalone to stack due to spanning tree recalculation and connectivity loss with the RADIUS server for approximately 10 to 30 seconds.
wi01223354/ ERS495900-189	In a scaled environment, with the maximum number of NEAP clients per port, it could be 30 seconds or more before the prompt returns after issuing the ACLI command **clear eapol non-eap**.
wi01224296/ ERS495900-209	Critical logs associated with exceptions are not sent to remote system log.
ERS495900-275	EDM: An error message is displayed when you try to add I-SID to a VLAN from EDM and SPBM is not enabled. You can add I-SID to a VLAN from CLI successfully when SPBM is not enabled.
ERS495900-248	Robustness: Router VRRP is disabled after AUR is performed on base unit
ERS495900-249	Robustness: Router VRRP is disabled after AUR is performed on base unit
ERS495900-575	802.1x Fail Open VLAN Continuity mode: IP phone is not authenticated using ADAC LLDP detection after Radius server fails and recovers.
ERS495900-581	4096-9216 bytes and Total Jumbo counters are not incremented on NNI interfaces if send traffic frame size is 9195-9198B.
ERS495900-738	ADAC: Error message appears when **adac op-mode untagged-frames-advanced** is issued first time after boot default.
ERS495900-819	Multicast traffic to BEB X is down or fluctuating for up to 25 seconds if NNI uplinks are down or up on BEB Y. BEB X and BEB Y receive the multicast traffic for the same groups.
ERS495900-833	It approximately takes 100 seconds for traffic (to 512 groups in 128 VLANs) to recover through alternative path after one Backbone Core Bridge (BCB) in the data path fails.
ERS495900-909	IP.cfg: USB config file is not copied after boot default and log appears that the USB config file is not found.
ERS495900-1068	There is inconsistency in **`show script`** command help menu. For example, 'Block' line from help menu starts with a lowercase and 'Block' line from help menu does not end with period.
ERS495900-1093	UBP: The switch does not apply the UBP filter if IPv6 FHS filter is installed first.
ERS495900-1492	When loading a verbose ASCII running configuration saved from a switch in SPB mode, the global and interface default **`eapol multihost fail-open-vlan`** commands fail.
ERS495900-1509	After enabling radius use-management-ip, there is an inconsistency between Telnet and SSH session regarding closing the sessions.
ERS495900-1603	ACLI PIPE: The find pipe filter displays the output of mem-show.

Table continues…

Change Request number	Description
ERS495900-2005	IPFIX: The **show ip ipfix table active-flows** command is not available for standalone unit.
ERS495900-2062	EDM: User password to access the switch can expire while using password aging time or command to change password at first login.
ERS495900-2650	Boot with ASCII Configuration file: The two blocks cannot have the same name. This incorrect condition is not detected when adding a boot script entry block but when booting from block 2, `% Invalid script entry` error message is displayed.
ERS495900-2658	Boot with ASCII configuration (boot script): Not all configurations can be applied using this feature. The script file must contain only commands which can be applied to the switch or stack in a defaulted state. The following configurations are not accepted because they first require a reboot to change the operating mode: • SPBM commands • STPG related commands • RSTP related commands Additionally, ssh and ssl commands in the configuration script fail because keys or certificates are not available when they need to be applied.

ERS495900-2664	The **show ip igmp sender** command displays only the following:
	• senders multicast source which is directly attached
	• SPBM I-SID to bridge multicast across the SPB cloud used by the switch
	The command does not display the multicast sources attached to the switch if a BEB is configured with L3 or IP Shortcut to route multicast traffic across the SPB cloud.
	Following is an example:
	`Switch#show i-sid`
	`I-SID Vid UNI-type Ports`
	`--------- ---- ----------- ------------`
	`10080 80 C-VLAN 8,56,66,76,99 <--- Vlan-80 has i-sid 10080`
	`Switch#show ip igmp sender`
	`Group Address Interface Member Address Port`
	`-------------- ---------- --------------- ----------`
	`235.100.80.1 80 100.100.80.1 0 <--- Multicast sources attached to vlan-80`
	`235.100.80.2 80 100.100.80.1 0`
	`235.100.80.3 80 100.100.80.1 0`

ERS495900-124	MSTP: MAC address in MSTP MSTI instance is not displayed in MAC address table.

Table continues…

Change Request number	Description
ERS495900-171	SPBM MHMV: After a base unit reset, reauthentication of all EAP and NEAP clients can take a few minutes.
ERS495900-332	SPBM MHMV: Error message `Can't set bseeGuestVlanEnabled` is displayed when GV is disabled on a stack with eapol enabled.
ERS495900-802	Auto SPBM: Incorrect error message is displayed when trying to enable SPBM while spanning-tree mode is set to RSTP.
ERS495900-1089	Error message is not displayed when SPBM is enabled while RSTP is configured on DUT.
ERS495900-1207	IGMP: Remote streams learned over NNI are displayed with port 0/0 in igmp sender table.
ERS495900-1373	Audit Log: An audit log message is not generated when the switch is configured with an IP.cfg file and management VLAN creation fails due to an invalid VLAN number specified in the IP.cfg file.
ERS495900-1521	`% RMON stats entry already exists` error appears while loading verbose rmon running-config.
ERS495900-1522	EDM/EDM Offbox: Eap settings are not autoconfigured when autoPortModeFaClient flag is enabled from EDM.
ERS495900-1709	SPBM+MHMV: Client from NBU does not update priority when re-authentication process is triggered manually.
ERS495900-1724	IPv6 interface is inaccessible when VLAN configuration control is automatic and NBU ports are removed and added back in the original VLAN.
ERS495900-1985	After reset, QoS traffic sets are corrupted on NBU ports if the installation process interacts with DHCP snooping over SPB or MGMT IPV6 over SPB.
ERS495900-2295	Log is not generated when FA table limit is reached for EAP topology.
ERS495900-295	AUR: LLDP settings are lost after AUR is performed on BU (renumber units scenario)
ERS495900-2522	The user role appears as `unknown` in the audit log when telnet access is enabled or disabled from non-base unit (NBU) console.
ERS495900-2540	During the following scenarios the IP address configuration for the last configured L3 VLAN interface is lost on a stack of three or more units: • If IP Shortcuts and the maximum number of L3 VLAN interfaces are configured. • If the stack running in temporary base unit mode is rebooted. • Stack reboot followed by a base unit reboot.
ERS495900-2546	Half duplex is not supported on ERS 59100 GTS and ERS 59100GTS-PWR.

Table continues…

Change Request number	Description
ERS495900-2577	NNI to NNI can be configured on stack or standalone containing 59100 units.
ERS495900-2342	SSH retry is not working when using other value than default one.
ERS495900-2631	Password change rate limiter allows the user to change the password (to access the DUT via console, SSH or telnet) one extra time per day to the configured value.
ERS495900-2634	If the base unit reboots in a stack configured with SPBM, IP Shortcuts, and DHCP Relay, you can lose the DHCP Relay settings on the management VLAN interface.
ERS495900-2637	Default username will not default the password aging time, inactive period, SSH and telnet access for a username.
ERS495900-2685	IP Shortcuts can be enabled without setting IP source address, which is not a valid configuration.
ERS495900-2686	If IP Shortcuts is enabled in an SPBM instance, it remains enabled after deleting the SPBM instance.
ERS495900-2690	In an SPBM with IP Multicast and IP Shortcuts environment, issuing the **`show ip igmp interface`** command displays 0.0.0.0 instead of querier IP. This is only a display issue.
ERS495900-2691	The switch does not list the UNI Receiver ports in the **`show isis spbm ip-multicast-route vlan <vlan_id> detail`** command output. This is only a display issue.
ERS495900-2712	Issuing the **`blink-leds`** command causes 1 GB SFP links to bounce. A link down event is noticed, followed immediately by a link up event.
ERS495900-2728	IP Shortcuts: The switch appears to be unreachable through NNI in traceroute if it is the first hop because TTL in IP packets are internally decremented twice.
ERS495900-2788	When SPBM is enabled and IS-IS overload is not set, ARP requests are not forwarded by the switch or stack to a non-SPBM device in the Management VLAN.
ERS495900-2802	Image download from USB fails with the following error message if the file is marked as read only: `% Error accessing image file, file missing or can't access USB device`
ERS495900-3105	SPBM: Cannot enable SPBM on 5900 stack where the ERS 59100 model is used as a Base Unit.

Chapter 5: Known issues and limitations

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

Known issues

This section identifies the known issues for the following products:

- Ethernet Routing Switch 4900 Series
- Ethernet Routing Switch 5900 Series

Table 9: Known issues

Change Request number	Description
Issues found in Release 7.3:	
ERS495900-3584	Lost ability to create VLANs 4001-4008 (reserved for MSTP) - working in 7.2.0 VLANs 4001-4008 cannot be created even if there are no MSTIs configured or if there are different values for MSTP reserved VLANs configured.
ERS495900–3353	Radius: Inconsistency between Global Radius and Radius used by EAP/Neap concerning the mgmt ip address used to send Radius messages while authenticating eap/neap clients. When only the global Radius server is used for authenticating eap or neap users both out-of-band and in-band management addresses are used as source for sending Radius messages by the switch. The address that is used depends on the routing table. If the route to reach Radius server uses out-of-band configuration than the out-of-band address is used; otherwise, the in-band management address is used. When different servers are configured for eap and neap authentication only the in-band address is used as source for the radius messages sent to the server.
ERS495900-3345	SPBM EAP: Traffic from authenticated NEAP users is sent in Guest VLAN and not in Initial VLAN when non-eap-use-radius-assigned-vlan is disabled.
ERS495900-3328	IPv6 Data Tunneling: sent traffic doesn't recover after bouncing source of one tunnel

Table continues…

Change Request number	Description
	In setups with multiple IPv6 tunnels configured with the same IPv4 source and having configured backup IPv6 Static Routed, the IPv6 static routes may not be restored correctly if bounce the source of one tunnel. WORKAROUND: Bounce IPV6 forwarding. The issue is not reproducible if no IPv6 backup routes configured or if the tunnels have different IPv4 source addresses.
ERS495900–3299	AUTO: Static Mroute for PIM: Direct route between DUTs does not take precedence over the static-mroute configured between DUTs
ERS495900-3256	IPSC with route-maps: Set-metric option does not work when redistributing routes into ISIS.
ERS495900–3239	Serious logging displayed: "Used stack size of task <taskname> is (2147483647%)". This is only a display issue and can be ignored.
ERS495900–3212	EDM: Inconsistency between EDM and EDM Offbox regarding Radius or TACACS authentication for serial or Web/Telnet.
ERS495900–3177	PVLAN: Inconsistency with legacy VLAN, if configcontrol is Automatic user is not permitted to move isolated port from one PVLAN to another without removing it from the first PVLAN.
ERS495900–3097	UBP: Unable to correctly install UBP if DHCP Snooping and ARP Inspection are enabled (SPB environment). WORKAROUND: The dhcp-snooping should be enabled on the initial vlan, before trying to authenticate the clients.
ERS495900–3059	SPBM Multicast: not all multicast traffic recovers after flushing igmp on source in a scenario with non-spbm device connected to BEB This is reproducible only after the groups are flushed multiple times. The traffic recovers after a period of time.
ERS495900–2987	EDM: If the next hop displayed in EDM for routes learned through IP Shortcuts is 127.x.x.x, it means it is an IP Shortcut next hop over the SPBM cloud. WORKAROUND: Use ACLI to display next hops.
ERS495900-2983 ERS495900-2982	Support COA in FA Mode: VLANs created by CoA Request are not deleted when stack transitions to standalone or when BU failover occurs with the FA client connected on BU. Failover scenarios, such as removing a unit from the stack, stack transition to standalone or vice-versa may result in not removing autocreated VLANs even if it has no members.
ERS495900–2933	EAP track all MACs :eap users in Held state not tracked after failing authentication because of UBP with high security. **`show eap summary`** command counts only authenticated EAP clients. For EAP clients in other states, double check with **`show eap sessions eap`** command.
ERS495900–2889	Console: bcmLINK.0 appears on console after closing all the interfaces.

Table continues…

Change Request number	Description
	This error might be seen intermittently. It can be safely ignored.
ERS495900–2836	More then 3 requests are sent to Primary Radius EAP server configured, although all the retries expired. When an EAP authentication occurs and the primary RADIUS server becomes unreachable during authentication process or just before, every packet must query primary first, wait for timeout and then try secondary. This situation occurs only for a short period of time, usually under 2 minutes, until the switch detects the primary RADIUS server as non-reachable. From this point, packets will go directly to the secondary RADIUS server.
ERS495900–2772	EDM: Error returned when viewing USB file list from EDM and the USB contains a big number of files. If a query of USB device using EDM or AFO returns error "The request timed out! The connection with the device may be lost or the device may be down". EDM/AFO utilize SNMP to retrieve the USB file structure, if the USB device is very full or has a complex file structure the SNMP response may timeout. A USB memory device with fewer files or less complex file structure will respond quicker, preventing the timeout condition.
ERS495900–2720	NVR CFG: Unexpected log is issued "NVR CFG - NVRAM file system check: errors detected. Please reboot the system!"
ERS495900–2713	If both In-band and Out-of-band management addresses are configured with RADIUS use-management-ip enabled, the source IP address in RADIUS packets sent by the switch are associated with the interface through which the packets are sent. If the RADIUS server is reachable through both interfaces, it is not always predictable which one will be selected for the source IP. If the source IP address is not known in the RADIUS server configuration, request packets are dropped. WORKAROUND: Configure the RADIUS server to allow both addresses. Both addresses must be added as RADIUS clients.
ERS495900–1359	SPBM EAP: When SPBM is enabled, EAP clients will not get authenticated if an invalid RADIUS Assigned VLAN is received from RADIUS Server.
ERS495900–1285	TDR test was not able to detect polarity when cross over cables are used.
Issues found in previous releases:	
ERS495900-3539	Ipv4 Mgmt over SPBM: Connectivity loss occurs after bouncing ip routing when IPv6 forwarding is enabled WORKAROUND: If IP routing needs to be bounced in this scenario, you must also bounce IPv6 global forwarding by entering the following ACLI commands, in this specific order: 1. no ip routing 2. no ipv6 forwarding 3. ip routing 4. ipv6 forwarding

Table continues…

Change Request number	Description
ERS495900-3514	IGMP with Roaming Multicast Source with SPB enabled currently does not work.
ERS495900-1440	EDM: In the Globals tab (path: Configuration ->IS-IS -> IS-IS), when only IpSourceAddressType is set, IpSourceAddress is set to a random IP address. This can be avoided by setting IpSourceAddressType and IpSourceAddress together.
ERS495900-2142	SNMP trap is not sent when Link State Tracking upstream port is down and the unit is in power off state. SNMP trap is sent when LST upstream port is up after the unit is powered on and bsLstInterfaceStatusChanged log message is added to the log list.
ERS495900-2202	Port mirroring VLAN: Control packets are mirrored on NNI interface even when the VLAN parameter from the configured instance is different.
ERS495900-2229	TFTP: `TFTP operation failed. Unknown reason.` error is displayed intermittently when copying the ASCII file on TFTP server. WORKAROUND: Retry to copy the ASCII file on TFTP server.
ERS495900-2243	When an invalid image is downloaded in an EDM Offbox session, error message `commitFailed` is displayed instead of `Invalid image.`
ERS495900-2316	If EAPOL is enabled on protocol VLAN ports, Ether2 User-Def traffic is not forwarded.
ERS495900-2391	EDM: Option to select Multicast VLAN Registration (MVR) application does not appear in the path **Configuration-** > **Edit** > **File System** > **Ascii Config Script Files**. WORKAROUND: Leave the Application field empty rather than using Select All in the dialog box. This is to ensure ASCII configuration contains MVR settings.
ERS495900-2455	Incorrect log message appears while moving NEAP clients to another VLAN.
ERS495900-2527	Storm Control: Sampling works poorly with minimum poll interval (default value), ports are blocked or unblocked even if the rate is constant and always under the high watermark. WORKAROUND: If high accuracy is required it is recommended to increase the "Poll interval" value. If small "Poll interval" is needed the values for High/Low watermarks should be adjusted to compensate for an error of +- 10 to 20 percent.
ERS495900-2538	When using PuTTY as an SSH client configured with 1 minute rekeying, SSH secured TCP remote Syslog session is unstable after running SNMP walk. The secured tunnels do not re-open and SSH session rekey does not happen every minute. WORKAROUND: Configure SSH client's session rekey parameter to an interval of at least 5 minutes.
ERS495900-2669	IP Shortcuts: Management uses IP source address instead of Management VLAN IP when ports are not assigned to Management VLAN and I-SID. WORKAROUND: Ensure at least one port is linked to VLAN to allow remote management of the device.

Table continues…

Change Request number	Description
ERS495900-2671	Boot with ASCII configuration: The **`show script block`** command output displays the last status with the value of failed for newly created entries even if there is no attempt to apply the scripts.
ERS495900-2711	SFP Port Led: EDM shows green when actual front panel light is amber for a 1 GB SFP module in 10 GB SFP+ port.
wi01187211/ ERS495900-18	If IS-IS adjacency is established over an MLT/LACP trunk, the information about IS-IS interfaces is displayed for both the trunk and its members in EDM and only for the trunk itself in ACLI.
ERS495900-44	SPBM L2VSN Stacking: SPBM MAC addresses on an MLT are not correctly displayed after disabling/enabling the MLT. The traffic is not affected.
ERS495900-64	SLA Mon: DSCP is reset to zero while performing NTR tests on CVLAN.
wi01206409/ ERS495900-82	SNMP users cannot be created from the EDM Offbox. WORKAROUND: Create SNMP users from EDM or ACLI.
ERS495900-89	EDM: Option to map VLANs in MSTP to MSTIs is not available.
wi01208072/ ERS495900-99	When a non-SPBM switch is connected to an SPBM switch and the Multiple Spanning Tree Protocol (MSTP) instances do not match, the in-band port from management VLAN is set to discarding mode instead of forwarding mode. WORKAROUND: Ensure all VLANs are in the Common and Internal Spanning Tree (CIST) for this scenario. See *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-502 for more information regarding MSTP.
wi01222464/ ERS495900-172	SSHC DSA/RSA key cannot be uploaded to USB from the non-base unit using NetSNMP. WORKAROUND: Set each MIB separately to ensure key file uploads successfully.
wi01222640/ ERS495900-176	When mapping a VLAN to a non-existent STG using EDM, the error message displays an incorrect STG number.
wi01223662/ ERS495900-194	EDM: In the Ascii Config Script Files screen in EDM, not all applications are available for selection for entries at the bottom of the screen due to the size of the pop-up window. WORKAROUND: Scroll the screen so that the entry is in the upper part of the EDM screen, or use ACLI to configure.
wi01223817/ ERS495900-197	In an SPBM environment, remote MAC addresses are not learned on the destination device after NNI ports are bounced on the source device. WORKAROUND: Bounce IS-IS on the source SPBM switch.
wi01224130/ ERS495900-204	When enabling link aggregation on a group of ports with inconsistent settings, an error is issued (‘% Ports have different IPSG configurations’) as expected. However, link aggregation is enabled partially on the list of ports, up to the first port with different settings.

Table continues…

Change Request number	Description
wi01224917/ ERS495900-219	In a stack in TBU mode, when using the serial console on the former base unit which left and rejoined the stack, some QoS UBP statistics (**show qos ubp statistics**) may be displayed as 0. WORKAROUND: Use the serial console on the temporary base unit or use telnet/SSH to view the correct QoS UBP statistics.
ERS495900-265	Adding classifier with meter to an existing set is not allowed even if resources are available.
ERS495900-301	Issuing a **`show interface config`** command from an SSH session does not display proper output and the cursor blocks when the terminal length is set to 0.
ERS495900-628	CFM Integration with IP Shortcut: EDM does not support L2 Ping IP and L2 Traceroute IP.
ERS495900-672	EDM: Changing QoS if-group on all ports is not possible (action is done only partially on some ports and errors are displayed.
ERS495900-832	CPU stays at 100% and traffic fluctuates for 125 to 150 seconds after the second NNI added on the DUT where the MC source is connected (MC traffic for 1024 groups in 256 VLANs).
ERS495900-1061	UBP GRIP 15329 and re-architecture: When UBP clients with 128 classifiers are added or removed, the following log message is generated even if the filter is removed from the port. "Unable to delete UBP filter set on interface."
ERS495900-1300	When setting a port as NNI, the switch does not display a warning message stating that it is recommended to remove the NNI ports from non-SPB VLANs or automatically remove the NNI interfaces from non-SPB VLANs
ERS495900-1460	EDM: There is inconsistency between CLI and EDM output for **`show flash history`** command.
ERS495900-1853	EDM: Option to default the port FA Message authentication key is not available in the ports tab (path: **Configuration** > **Edit** > **Fabric Attach**). WORKAROUND: Use CLI to default the Authentication Key.

Limitations and considerations

The following table lists known limitations and considerations:

Item	Applicable Product	Description
1	ERS 5900 Series	Some terminal programs can cause the Console Interface to crash if you enter a RADIUS secret containing the character “k”. The issue has been reproduced using Tera Term Pro (version 2.3), as well as Minicom (version 2.1) on a Linux system.

Table continues…

Item	Applicable Product	Description
	ERS 4900 Series	
2	ERS 5900 Series ERS 4900 Series	Avoid using MAC security on a trunk (MLT).
3	ERS 5900 Series ERS 4900 Series	Failed attempts to log in (using TACACS+ authentication and accounting) are not stored in the accounting file.
4	ERS 5900 Series ERS 4900 Series	When switches are in Multiple Spanning Tree Protocol (MSTP) mode and connected using a trunk (MLT), and at least one MSTI is configured, the switch can return an incorrect STPG root if you change the mode to STPG and reset the switches.
		MSTP is the default spanning tree mode. When using the switch with SPB enabled, MSTP will not converge if used in the same MSTP region with switches that are not running SPB. This is not an issue if all VLANs are in the common and internal spanning tree (CIST).
5	ERS 5900 Series ERS 4900 Series	While downloading the image file, you may receive the following error message: "Error reading image file." WORKAROUND: Typically, this issue can be resolved by simply restarting the image download. If this does not resolve the issue, Avaya recommends that you try an alternate method to download the image to the switch (that is, the Web Interface).
6	ERS 5900 Series ERS 4900 Series	The IPFIX sampling data rate cannot be changed because of a related hardware limitation.
7	ERS 5900 Series ERS 4900 Series	Demo License to enable OSPF, ECMP, VRRP, and IPFIX is for a period of 60 days. The trial license expires at the end of the 60 day period and the features are disabled. The system sends traps advising of license expiration. Demo license expiry traps: • Five days prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 5 day(s). • One day prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 1 day(s). • At termination of demo license: bsnTrialLicenseExpiration: Trial license 1 has expired.
8	ERS 5900 Series	Do not enable IP Source Guard on trunk ports.

Table continues…

Item	Applicable Product	Description
	ERS 4900 Series	
9	ERS 5900 Series ERS 4900 Series	Non-existent VLAN Mapping for MSTI: EDM/SNMP support for VLAN Mapping for MSTI is not available.

10	ERS 5900 Series
	ERS 4900 Series
		You cannot enable MAC Security on LACP enabled ports. The following message displays:
		`%Cannot modify settings`
		`%MAC Security status cannot be modified. Disable LACP first.`

11	ERS 5900 Series ERS 4900 Series	Rate Limiting: When you have the following scenario: 1. rate-limiting is performed at 10% (or by setting any percent value threshold) 2. the speed ratio between the inbound port and the client port is 10:1 (for example 10Gbps inbound link and 1Gbps client port link) 3. inbound broadcast or multicast traffic throughput on the inbound link is more than 10% link-rate speed then the client port will receive 0.1 * [inbound traffic rate] and not the expected 1Gbps broadcast or multicast traffic. Example: • inbound port link rate = 10Gbps , client outbound link rate = 1Gbps , rate limiting set to both at 10% • inbound traffic rate = 3Gbps broadcast traffic The actual client traffic received rate = 333Mbps and not the expected 1Gbps
12	ERS 5900 Series ERS 4900 Series	In a stack configuration, SSHC configuration options are only available from the base unit

13	ERS 5900 Series
	ERS 4900 Series
		When you manually create an LLDP MED network policy, LLDP checks that the specified VLAN ID corresponds to a voice VLAN created inside the VLAN application. If the VLAN is not a voice VLAN or the VLAN does not exist, the switch displays a warning message. The switch creates the policy even if the VLAN is not voice enabled or does not exist. The switch may display one of the following messages:
		`% Policy will be set on port x with vlan-id of a non-existent vlan y`
		`% Policy will be set on port x member of the non-voice vlan y`

Table continues…

Item	Applicable Product	Description
14	ERS 5900 Series ERS 4900 Series	If you configure a stack of three or more units in Both Directions, (the stack is cabled in a non-ring configuration and the missing cable is between two non-base units) there will be no temporary base unit election in case the base unit fails. In this scenario, the stack will break and the base unit cannot be replaced and its CFG image will not be mirrored. In addition, the base unit is not present in the AUR cache, so the base unit will not be ready for replacement, and its MAC address cannot be displayed or removed.
15	ERS 5900 Series ERS 4900 Series	In a ring stack, of four or more units, if rebooting or powering off a unit that is not directly connected to the base unit, the stack will be configured in Both Directions configuration (the stack is cabled in a non-ring configuration and the missing cable is between two non base units). In this scenario there will be no temporary base unit election in case the base unit fails. If the base unit fails, the stack will break, so the base unit cannot be replaced, and its CFG image will not be mirrored. In this case the base unit is not present in the AUR cache, so the base unit will not be ready for replacement, and its MAC address cannot be displayed or removed, as long as the stack remains in this state.
16	ERS 5900 Series ERS 4900 Series	The area ID 0.0.0.0 is created by default and it is reserved for the backbone area. Error message is displayed when you create area ID 0.0.0.0 on the switch using ACLI or EDM. For example, the following error message is displayed on ACLI when the command area 0.0.0.0 is entered: `% Cannot modify settings% Can't delete or modify backbone area`
17	ERS 5900 Series ERS 4900 Series	In order for EAP to work with SPBM configurations, all VLANs used by EAP should be SPB VLANs (C-VLANs), including initial VLANs, Guest VLAN, Fail Open VLAN, VoIP VLANs, RADIUS Assigned VLANs, and ADAC Voice VLANs (in the case where ADAC authentication is used).
18	ERS 4900 Series	The ACLI command, **show stack-cable-info** is not available in ERS 4900 Series. Information about the stack cables cannot be viewed.
19	ERS 5900 Series ERS 4900 Series	From Release 7.2, DHCP relay is disabled by default.
20	ERS 5900 Series ERS 4900 Series	Multiple bindings are not supported in MHSA on FA Server.

VLACP issue

In some situations, when you use VLACP the switches remove a link from service due to variations in the arrival time of VLACP messages (VLACP PDUs) from the far end. The issue can exist

between the ERS 5900 or ERS 4900 models and ERS 8300 and ERS 8600 models when the system runs short timers with a default timeout interval of 3 time-outs or less. The switches maintain a rolling history of the last 3 received VLACP PDUs (by default) and calculate the time variance across and between these VLACP messages.

SOLUTION: Increase the VLACP timeout-scale value to 3 or more.

Filter resource consumption

Applications consume filter resources, which are a combination of masks and filters, also known as rules.

A filter specifies the bit pattern to match.

A mask specifies the bit position to match and the evaluation precedence of the filters.

To enable some applications, for example Port Mirroring and IGMP, a set number of masks and filters are required.

The following table summarizes the applications that require mask and filter resources.

Table 10: Application mask and filter resource requirements

Application	Category	Masks required	Filters required
Broadcast ARP and ARP Inspection	Non QoS	1	1[a]
DHCP Relay or DHCP Snooping	Non QoS	1	4[a]
QoS (default untrusted policy)	QoS	2	2[a]
QoS (DAPP with status tracking)	QoS	1	1[a]
QoS (Auto QoS)	QoS	1	4[a]
Port Mirroring (MAC based, xrxytx)	Non QoS	1	2[a]
EAP Authetication (EAPoL packet filter)	Non QoS	1	2[a]
IPFIX	Non QoS	1	1[a]
ADAC	Non QoS	1	1[a]
RIP	Non QoS	1	1[a]
UDP Broadcast	Non QoS	1	1[a]
VRRP	Non QoS	1	1[a]
OSPF	Non QoS	1	1[a]

Table continues…

Application	Category	Masks required	Filters required
Content Based Forwarding	Non QoS	1	up to 16[a]
IP Source Guard	Non QoS	1	11[a]
PIM	Non QoS	1	2[a]
SPB	Non QoS	1	1[a]
SPB - DHCP	Non QoS	1	6[b]
SPB - CFM	Non QoS	2	2[a]
IGMP	Non QoS	up to 2	1[c]
MLD	Non QoS	up to 2	1[c]
FHS	Non QoS	1	24[b]
IPv6	Non QoS	1	1[a]
IPv6 over SPBM (when IPv6 Forwarding is enabled)	Non QoS	up to 3	1[a]
Private VLAN	Non QoS	1	1[b]
Notes: **a**: number of filters required per port **b**: number of total filters **c**: number of filters required per VLAN enabled plus one common filter per mask (i.e. 256 VLANs enabled require two masks with 256 filters on first mask and two filters on second mask)			

On the switch, the resources are shared across groups of ports. For each group of ports, 16 masks are available, with 256 filters available for each mask. By default, the system consumes one mask with one filter per port for ARP. This leaves 15 masks available, each with 256 filters for QoS and other non QoS applications to configure dynamically.

You can use the **`show qos diag`** command to assess the current filter resource usage for each port on the switches.

The **`show qos diag`** command displays the number of QoS masks and filters and non QoS masks and filters consumed on each port. You can determine whether an application that requires filter resources can be enabled on a port by verifying that the number of available masks and filters meets the mask and filter requirements of the application.

On the switch, you can count the unused masks to determine the number of available masks for a port by using the output of the **`show qos diag`** command. The switches share resources across a group of ports. The filters used by QoS or non QoS applications on a port for a specific mask determine the available filters for that mask for all ports from that group.

On the switch, you can determine the number of filters available for a mask from a group of ports by adding the total number of QoS and non QoS filters in use and subtracting that number from 256. If the number of filters in use for a mask equals 256, you cannot use that mask on other ports from the same group.

Note:

Maximum eight precedences can be used with meter for QoS policies or Non-QoS applications. Using **show qos diag** command, you can view total number of precedences (from 16 to 1) and check the QoS and Non-QoS meters used. By default, ARP uses meters on precedence 16. If the other seven precedences are using meters (QoS and Non-QoS) then no other precedence can be used with meter (QoS and Non-QoS) .

Example - IP Source Guard on an switch port

On the switch, you need 1 mask and 11 filters to enable IP Source Guard on a port. When you view the **show qos diag** command output you see that port 5 is currently using a total of 4 masks. IP Source Guard uses the next available mask and, from the command output, you can see that there are 256 filters available for mask 14. So you can enable IP Source Guard.

Flow Control

The default value for flow control is asymmetric/asymm-pause-frame (forced settings / auto-negotiation advertisement).

Example

Disabling flow control when auto-negotiation is enabled:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface ethernet 7-8
Switch(config-if)#auto-negotiation-advertisements port 7 1000-full
Switch(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
---- ---------------------------------------------------------------
7                                 1000Full
8    10Full        100Full        1000Full           AsymmPause
Switch(config-if)#show interfaces 7-8
              Status                      Auto                       Flow
Port Trunk  Admin  Oper Link LinkTrap Negotiation  Speed   Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
7          Enable  Down Down Enabled  Custom
8          Enable  Down Down Enabled  Enabled
```

Enabling asymmetric flow control when auto-negotiation is enabled:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface ethernet 7-8
Switch(config-if)#$iation-advertisements port 7 1000-full asymm-pause-frame
Switch(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
---- ---------------------------------------------------------------
7                                 1000Full           AsymmPause
8    10Full        100Full        1000Full           AsymmPause
Switch(config-if)#show interfaces 7-8
              Status                      Auto                       Flow
Port Trunk  Admin  Oper Link LinkTrap Negotiation  Speed   Duplex Control
---- ----- ------- ---- ---- -------- ----------- -------- ------ -------
```

```
7           Enable  Down Down Enabled  Custom
8           Enable  Down Down Enabled  Enabled
```

Disabling flow control when auto-negotiation is disabled:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface ethernet 7-8
Switch(config-if)#duplex port 7-8 full
Switch(config-if)#flowcontrol port 7-8 disable
Switch(config-if)#show interfaces 7-8
               Status          Auto                        Flow
Port Trunk Admin  Oper  Link Negotiation  Speed  Duplex Control
---- ----- ------ ----  ---- -----------  -----  ------ -------
7           Enable Up    Up   Disabled     1000Mbps Full Disable
8           Enable Up    Up   Disabled     1000Mbps Full Disable
```

Enabling asymmetric flow control when auto-negotiation is disabled:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface ethernet 7-8
Switch(config-if)#flowcontrol port 7-8 asymmetric
Switch(config-if)#show interfaces 7-8
               Status          Auto                        Flow
Port Trunk Admin  Oper  Link Negotiation  Speed  Duplex Control
---- ----- ------ ----  ---- -----------  -----  ------ -------
7           Enable Up    Up   Disabled     1000Mbps Full Asymm
8           Enable Up    Up   Disabled     1000Mbps Full Asymm
```

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 4900 and 5900 Series*, NN47211-103.

For more information on new features of the switch and important information about the latest release, see *Release Notes for Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-400.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 4900 and 5900 Series*, NN47211-505.

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

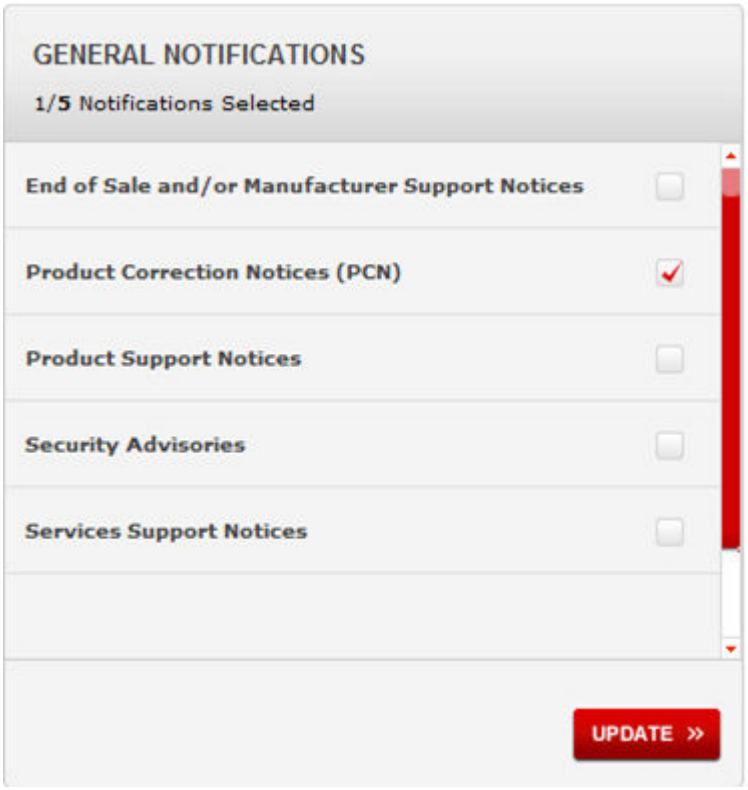
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

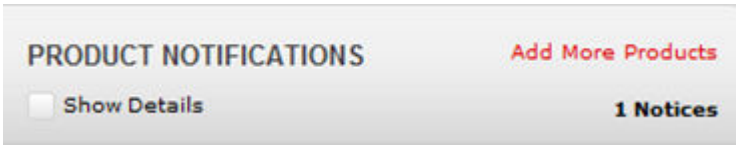
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services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

Procedure

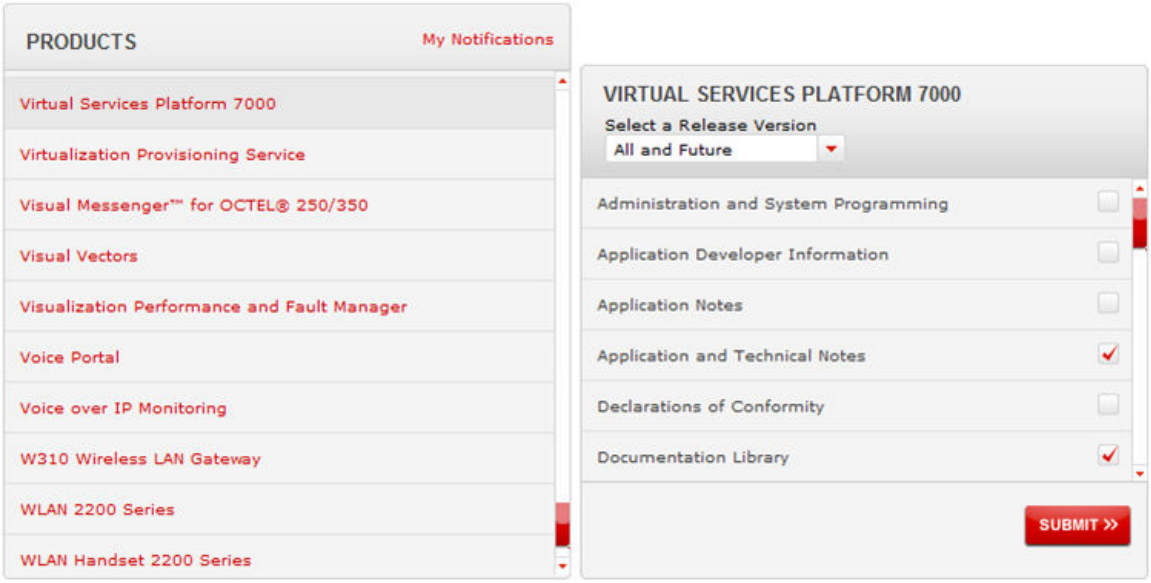
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click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