Release Notes for Avaya Ethernet Routing Switch 5900 Series

impose greater restrictions on You than the applicable Third Party Terms.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://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, 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 Avaya Ethernet Routing Switch 5900 Series.

These release notes provide the latest information about the current software release, as well as operational issues not included in the documentation.

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

Related resources

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 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 5900 Series*, NN47211-400.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 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/.

1. 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**.
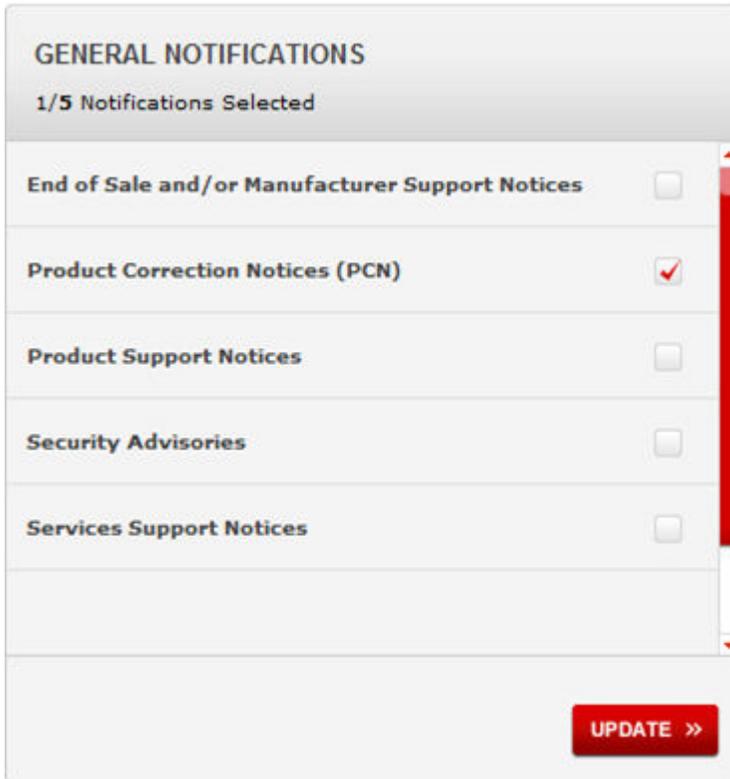
6. Click **OK**.

7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.
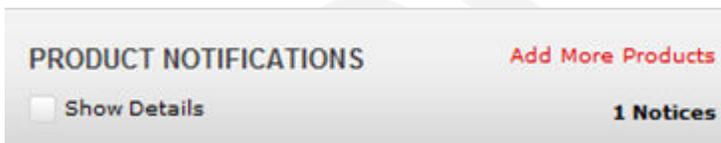
8. Scroll through the list, and then select the product name.

9. Select a release version.

10. Select the check box next to the required documentation types.

2   11. Click **Submit**.

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.

Chapter 2: New in this release

The following sections detail what is new in *Release Notes for Avaya Ethernet Routing Switch 5900 Series*, NN47211-400 for Release 7.0.1.

Features

See the following sections for information about the new features.

Fabric Attach updates

Following are the Fabric Attach changes:

Fabric Attach Server and Fabric Attach Proxy functionality

The switch supports Fabric Attach Server and Fabric Attach Proxy functionality. A Fabric Attach Server is an SPB capable network device connected to the fabric edge running the FA agent in FA Server mode. FA Servers receive requests to create services with specific I-SID/VLAN bindings. A Fabric Attach Proxy is a device running the FA agent in FA Proxy mode. FA Proxies support I-SID/VLAN assignment definition and have the ability to advertise these assignments for possible use by an FA Server, if connectivity permits. If FA Proxy is linked to FA Server in SPBM provisioning mode, then FA server needs to be a VSP 4000 or VSP 8000 Series unit.

Fabric Attach Auto Provision

You can use Auto Provision with an FA Server-capable device to take advantage of Fabric Attach functionality in non-SPB environments. Auto Provision allows an FA Proxy device (that is also FA Server-capable) to function as an FA Server when SPBM is disabled. With Auto Provision you can designate the device as an FA Proxy or FA Server. FA VLAN definitions, configured locally on an FA Proxy or through client processing, transparently replace I-SID/VLAN binding definitions in this scenario and allow all of the automated FA processing, with the exception of switched UNI-related operations, to be performed in the absence of SPBM operations. All existing FA default settings remain unchanged.

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

ACLI commands

This feature introduces the following ACLI commands:

- `fa auto-provision`

- **`default fa auto-provision`**
- **`fa proxy`**
- **`default fa proxy`**
- **`no fa proxy`**
- **`fa auto-provision proxy`**
- **`show fa elements client-type`**
- **`show fa zero-touch-options client-data`**
- **`fa zero-touch-options auto-port-mode-fa-client client-type`**
- **`fa zero-touch-options auto-pvid-mode-fa-client client-type`**
- **`no fa zero-touch-options auto-port-mode-fa-client client-type`**
- **`no fa zero-touch-options auto-pvid-mode-fa-client client-type`**
- **`fa zero-touch-options auto-port-mode-fa-client client-type <6-17>`**
- **`fa zero-touch-options auto-pvid-mode-fa-client client-type <6-17>`**
- **`fa zero-touch-options auto-trusted-mode-fa-client client-type <6-17>`**

RADIUS attributes

The switch supports two new RADIUS attributes for both EAP and NEAP authentications: Called-Station-Id and Calling-Station-Id. Calling-Station-Id represents the client MAC address. Called-Station-Id represents the switch MAC address.

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

Overview of features and hardware models by release

This section provides an overview of the Ethernet Routing Switch 5900 series software features and hardware models introduced in Releases 7.0

Features for Releases

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

Features	New in release
	7.0
802.1AB (Link Layer Discovery Protocol)	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	
802.1AB Avaya PoE Conservation Level Request TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB Avaya Call server TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB Avaya File server TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB Avaya 802.1Q Framing TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB Avaya Phone IP TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB customization For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB integration For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB (LLDP) MED Network Policy CLI For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB MED support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
802.1AB location TLV For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
802.1AB new default parameters For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x

Table continues…

Features	New in release
	7.0
802.1D Compliancy Support For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
802.1X-2004 support For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1X non-EAP Accounting For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1X non-EAP re-authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1X or Non-EAP and Guest VLAN on same port For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1X or Non-EAP with Fail_Open VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1X or Non-EAP with VLAN name For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1X or Non-EAP use with Wake on LAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1X RFC3576 For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1x multiple host single authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.1x NEAP support (MAC authentication) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
802.3at LLDP based discovery	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	
ADAC (including 802.1ab support) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
ADAC and Auto QoS Interoperability	x
ADAC Uplink over SPBM For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
ASCII configuration file generator For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Using ACLI and EDM on Avaya Ethernet Routing Switch 5900 Series*, NN47211-104.	x
ASCII Download Enhancements For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
ASCII script config support	x
Automatic Unit Replacement For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 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 5900 Series*, NN47211-700.	x
AUR enhancement For more information, see *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Automatic QoS and 802.1AB MED Interoperability For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
Autosave configuration enhancement For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Autotopology (802.1ab, SONMP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x

Table continues…

Features	New in release
	7.0
Boot/DHCP address assignment (RFC 1542)	x
Avaya Identity Engines Ignition Server For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Backup CONFIG file For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501, *Troubleshooting Avaya Ethernet Routing Switch 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.	x
boot partial-default command For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
BOOTP and DHCP RELAY For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
Boot/DHCP address assignment (RFC 1542)	x
BPDU filter For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x
Broadcast rate limiting	x
Change RADIUS Password For more information about the configuration, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Circuitless IP For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
Avaya Command Line Interface (CLI) For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 5900 Series*, NN47211-104.	x
CLI list command For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 5900 Series*, NN47211-104.	x
Configure asset ID	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	
CPU utilization For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503	x
Custom Autonegotiation Advertisement (CANA) ⊛ **Note:** ERS 5900 supports only full-duplex operation. For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Default all EAP settings For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Default IP For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
DHCP Client For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501, *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
DHCP Option 82 Support For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
DHCP Snooping For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
DHCP snooping external save For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Distributed MultiLink Trunking (DMLT) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Dual Syslog Server Support	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	
Dynamic ARP inspection For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Dynamic Route Table Allocation For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
EAP Fail Open with multi-VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
EAP and NEAP separation For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
EAP and non-EAP MultiVLAN capability For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
EAP-MD5 authentication For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
EAPoL Multihost MAC-max For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
EAPoL (802.1x) MHSA/MHMV and Guest VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Energy Saver For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x
Disable CLI audit log command For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Equal Cost MultiPath (ECMP)	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506	
Enterprise Device Manager For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 5900 Series*, NN47211-104.	x
EDM improved download support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Extended IP Manager For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Extended password history For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Fabric Attach For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 5900 Series*, NN47211-507.	x
Factory default command	x
Fail Open VLAN Continuity mode For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Show FLASH History For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Flow Control on gigabit Ethernet ports (802.3x) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Inactivity time out For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Improved syslog capabilities For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
Independent VLAN Learning (IVL) support	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502 .	
Internet Group Management Protocol version 2 (IGMPv2, RFC 2236) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
Internet Group Management Protocol (IGMP) Querier For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
Internet Group Management Protocol (IGMP v1/v2) Snooping and Proxy For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
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.	x
IPFIX For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and*Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x
IP local and static routes For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
IP Phone Automatic PoE Changes For more information, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 5900 Series*, NN47211-105.	x
IP Source Guard For more information, see *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
IPv6 Automatic Address Assignment For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
IPv6 First Hop Security For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
IPv6 management	x

Table continues…

DRAFT—November 4, 2015—4:41 AM (UTC)

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

Table continues…

Features	New in release
	7.0
For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	
MAC security port lockout For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Many to Many Port Mirroring For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
Multi-Link Trunking For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
MLT/DMLT/LAG Dynamic VLAN Changes For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
MLT and LAG Scaling For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
MLT enable/disable whole trunk (MLT shutdown ports on disable) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
Multicast over SPB For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 5900 Series*, NN47211-507.	x
Multicast Listener Discovery (MLD) snooping For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
Multiple local RW and RO user accounts For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
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 5900 Series*, NN47211-502.	x

Table continues…

Features	New in release
	7.0
NEAP IP Phone support	x
NEAP not member of VLAN For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Network Time Protocol (NTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
New unit quick to config For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Non-Local Static Routes For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
Non-unicast hashing over MLT/DMLT/LAG For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
Open Shortest Path First For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
Out-of-band management For more information, see *Quick Start Configuration for Avaya Ethernet Routing Switch 5900 Series*, NN47211-500.	x
Password change via EDM For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Ping command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Ping Source Address For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Port-based VLAN support For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring VLANs, Spanning Tree, and*	x

Table continues…

Features	New in release
	7.0
Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series, NN47211-502.	
Port mirroring (including ingress and egress) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
Port operational status enhancements For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
Protocol-based VLAN support (including IPv6 protocol VLANs) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
Protocol Independent Multicast-Sparse Mode (PIM-SM) For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
QoS - Diffserv Code Points (DSCP RFC2998) marking and classification For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
Quality of Service (QoS) - 802.1q For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
Quality of Service (QoS) - Layer 2 to Layer 4 filtering and policies For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
Quality of Service (QoS) - Offset filtering (first 80 bytes) For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
QoS IP/L2 Filter Options For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
QoS Queue Set Support For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
QoS queue statistics For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x

Table continues…

Features	New in release
	7.0
Quick start command and Web interface For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Remote Authentication Dial-In User Server (RADIUS) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
RADIUS Accounting Enhancements (RFC2866) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
RADIUS Assigned VLAN update for 802.1x - use most recent RADIUS VLAN enhancement For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
RADIUS Server Reachability For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
RADIUS EAP or non-EAP requests from different servers For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
RADIUS Management Accounting with TACACS+ support For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
RADIUS Request use Management IP For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
RADIUS NEAP password configurable key For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Rapid Spanning Tree Protocol (802.1w) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
Reload command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Remote Monitoring (RMON)	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503	
Remote Switch Port ANalyzer For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
Resilient stacking	x
RMON scaling For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
RO user access to telnet and SSH For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Routing Information Protocol For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
Routing Policies For more information, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506.	x
RSTP traps For more information, see *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
RSTP SNMP traps For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Run IP Office Script For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Run Scripts For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Running Configuration ACLI Display Commands For more information, see *ACLI Commands Reference for Avaya Ethernet Routing Switch 5900 Series*, NN47211-105.	x
Secure File Transfer Protocol (SFTP)	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	
Secure Shell (SSH, SSHv2) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
SFTP License and DHCP external support For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 5900 Series*, NN47211-104 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Show Environmental For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
Show flash function For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
show ip netstat For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Show Port enhancement For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503 and *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Show Software Status For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Show VLAN interface verbose command For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
Shutdown command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
SLAMon Agent For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
SLA Monitor	x

Table continues…

DRAFT—November 4, 2015—4:41 AM (UTC)

Features	New in release
	7.0
For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	
SLPP Guard For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
Simple Network Management Protocol (SNMP, SNMPv3) For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Configurable SNMP trap port For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
SNMP Trap enhancements For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
SNMP traps for DHCP snooping/DAI/IPSG For more information, see *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Simple Network Time Protocol (SNTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Software Licensing For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 5900 Series*, NN47211-104.	x
Spanning Tree Protocol Group (802.1D, 802.1t) For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
SPBM For more information, see *Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 5900 Series*, NN47211-507.	x
SSH Client For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
SSH RSA Authentication	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	
Stack counters For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
Stack monitor For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 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.	x
Stack Forced Mode For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Stack health check For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Stack Health Monitoring and Recovery For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503.	x
Stack loopback tests For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x
Static FDB MAC Entry For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
Sticky MAC Address For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Storm control For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
STP BPDU filtering ignore-self For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x

Table continues…

Features	New in release
	7.0
Syslog Support for 802.1X/EAP/NEAP/UBP For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
TACACS+ For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Telnet server and client For more information, see *Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference*, NN47216–600.	x
Terminal Mode Permanent Setting	x
Time Domain Reflectometer For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Trace Functions For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 5900 Series*, NN47211-503 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Trace Support for 802.1X For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Traffic Profile Filter Set Support For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504.	x
Trivial File Transfer Protocol (TFTP) For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501.	x
Disable USB and console For more information, see *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
User Based Policies For more information, see *Configuring Quality of Service on Avaya Ethernet Routing Switch 5900 Series*, NN47211-504 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	x
Username password enhancement	x

Table continues…

Features	New in release
	7.0
For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505.	
Virtual LACP For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
VLAN Scaling	x
Voice VLAN Integration For more information, see *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502.	x
Web User Interface (http and https)	x
WebUI MIB Web Page	x
WebUI Trap Web Page	x
Write memory and save config command For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Using ACLI and EDM on Avaya Ethernet Routing Switch 5900 Series*, NN47211-104	x
Ability to set password, username and type of security for any switch in stack For more information, see *Using ACLI and EDM on Avaya Ethernet Routing Switch 5900 Series*, NN47211-104 and *Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505	x
Auto Detection Auto Configuration (ADAC) - modify the 802.1AB detection mechanism used in ADAC to work correctly with the Avaya IP handsets	x
Increase PoE power For more information, see *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501 and *Troubleshooting Avaya Ethernet Routing Switch 5900 Series*, NN47211-700.	x

1 **Hardware models**

2 The following table provides a listing of the hardware models.

Switch model	Part number	Description
ERS 5928GTS	AL590001X-E6	ERS 5928GTS with base software license, no fans, no power supply unit (PSU), no power cord
	AL5900A1B-E6	ERS 5928GTS with base software license, two fan tray modules, back to front 450 Watt PSU, no power cord
	AL5900A1F-E6	ERS 5928GTS with base software license, two fan tray modules, front to back 450 Watt PSU, no power cord

Table continues…

Switch model	Part number	Description
ERS 5928GTS-PWR+	AL590002X-E6	ERS 5928GTS-PWR+ with base software license, no fans, no PSU, no power cord
	AL5900A2B-E6	ERS 5928GTS-PWR+ with base software license, two fan tray modules, back to front 1400 Watt PSU, no power cord
	AL5900A2F-E6	ERS 5928GTS-PWR+ with base software license, two fan tray modules, front to back 1400 Watt PSU, no power cord
ERS 5952GTS	AL590003X-E6	ERS 5952GTS with base software license, no fans, no PSU, no power cord
	AL5900A3B-E6	ERS 5952GTS with base software license, two fan tray modules, back to front 450 Watt PSU, no power cord
	AL5900A3F-E6	ERS 5952GTS with base software license, two fan tray modules, front to back 450 Watt PSU, no power cord
ERS 5952GTS-PWR+	AL590004X-E6	ERS 5952GTS-PWR+ with base software license, no fans, no PSU, no power cord
	AL5900A4B-E6	ERS 5952GTS-PWR+ with base software license, two fan tray modules, back to front 1400 Watt PSU, no power cord
	AL5900A4F-E6	ERS 5952GTS-PWR+ with base software license, two fan tray modules, front to back 1400 Watt PSU, no power cord

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

Chapter 3: Important notices and new features

This section describes important software and hardware related notices.

The ERS 5900 warranty includes access to software updates for features and maintenance releases.

Feature document location

The following table contains a list of key software features and their location in the documentation suite.

Table 1: Where to find information about key software features

Feature	Document
Custom Autonegotiation Advertisements (CANA)	✱ **Note:** ERS 5900 supports only full duplex operation. *Configuring Systems on Avaya Ethernet Routing Switch 5900 Series*, NN47211-501
EAPoL Multiple Hosts with Multiple VLANs (EAP MHMV)	*Configuring Security on Avaya Ethernet Routing Switch 5900 Series*, NN47211-505
Fabric Attach	*Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 5900 Series*, NN47211-507
Multicast over SPB	*Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 5900 Series*, NN47211-507
SPBM with EAP MHMV	*Configuring Avaya Fabric Connect on Avaya Ethernet Routing Switch 5900 Series*, NN47211-507
Non-unicast traffic over MLT	*Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502
IGMP and Multicast Flood Control	*Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 5900 Series*, NN47211-506

Release file names

The following table describes the Avaya Ethernet Routing Switch 5900 Series software components for this release.

Table 2: Software components

File Type	Description	File Name	File Size (bytes)
Secure runtime image	Standard SSH image for the Ethernet Routing Switch 5900 Series	5900_701017s.img	16,660,756
Diagnostic software version 7.0.0.3 and 7.1.0.4	ERS 5900 diagnostic software	5900_70003_diags.bin 5900_71004_diags.bin	6,143,204

> ⊛ **Note:**
>
> Units with diagnostic software versions 7.0.0.3 and 7.1.0.4 work with agent version 7.0.1.
>
> For example, if there is a unit with diagnostic software version 7.0.0.3, it need not be upgraded to diagnostic software version 7.1.0.4.

Boot Loader version 7.0.0.3	Bootloader image for ERS 5900	5900_70003_boot.bin	524,288
Enterprise Device Manager Help Files	EDM Help files zip	ers5000v701_HELP_EDM.zip	1,811,591
MIB Definition File	MIB Definition File	Ethernet_Routing_Switch_5900_MIBs_7.0.1.zip	1,467,892
COM Plug in	ERS 5900 plugin for COM	ers5900v7.0.1.0.zip	3,317,266

Software upgrade

The procedures in this section are used to upgrade the diagnostic and agent software.

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 <ip_address> diag <image_name> [no-reset] [usb]` 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 <ip_address> {primary | secondary} {image <image_name> | image-if-newer <image_name> | poe_module_image <image_name>} [no-reset] [usb]** 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.

Table continues…

Parameter	Description
	• 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.

Upgrading the PoE+ firmware

About this task

Upgrade the PoE+ firmware to the latest version on all PoE+ units.

Before you begin

Verify the PoE+ firmware version using command `show sys-info`. In the command output, check `PoE Module FW`. In a stack, to view this information for a specific unit, connect to the serial console of that unit.

Procedure

1. Do any one of the following to upgrade the POE+ firmware:

   • To upgrade the PoE+ firmware from TFTP, enter the following command:

   ```
   download [ address <TFTP server address> ] poe_module_image
   5900_poe_v15010.bin
   ```

   OR

   • To upgrade the PoE+ firmware from an USB storage device, enter the following command:

   ```
   download usb poe_module_image 5900_poe_v15010.bin [ unit <unit
   number> ]
   ```

2. The switch or stack reboots after the firmware is successfully downloaded and saved to the PoE+ board.

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 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

Supported software and hardware capabilities

The following table lists the known limits for the Avaya Ethernet Routing Switch 5900 Series, Release 7.0.1, and Enterprise Device Manager.

Table 3: 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	Maximum Number Supported in ERS 5900 series
Egress queues	Configurable 1–8
MAC addresses	32,768 ★ **Note:** Each MAC Security MAC configured uses two entries in the table, thus reducing the maximum number of MAC addresses that can be learned.
MAC Filtering list	128
Stacking bandwidth per unit	84 Gbps (42 Gbps up, 42 Gbps down)
Stacking bandwidth (full stack of 8 units)	Up to 672 Gbps
QoS precedence	16 per ASIC
QoS rules per ASIC	256 rules per precedence
Maximum number of units in a stack	8
Layer 2	
Concurrent VLANs	1,024
Supported VLAN IDs	1 - 4094 (0 and 4095 reserved; 4001 reserved by STP; 4002-4008 reserved by multiple STP groups)
Protocol VLAN types	7 Depending on the protocol specified, the number of protocol VLANs supported at one time varies between 3–7. See *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5900 Series*, NN47211-502 for more information.
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32
Maximum MAC Learning rate on an MLT trunk	500 new MAC addresses per second
Links or ports for MLT, DMLT or LAG	8
Static MAC Addresses	1,024
Spanning Tree Group instances (802.1s)	8
Avaya Spanning Tree Groups	8
DHCP Snooping table entries	1,024 per unit
Layer 3	
IP Interfaces (VLANs or Brouter ports)	256
ARP Entries total (local, static & dynamic)	4,096

Table continues…

Feature	Maximum Number Supported in ERS 5900 series
ARP Entries — maximum local (IP interfaces per switch/stack)	256
ARP Entries — maximum static	256
ARP Entries — dynamic	4,096 - (local + static)
IPv4 Routes total (local, static & dynamic)	4,000
IPv4 Static Routes	512
IPv4 Local Routes	254 (256 - 2 used internally by the system)
IPv4 Dynamic Routes (RIP & OSPF)	4,000 - (local + static)
Dynamic Routing Interfaces (RIP & OSPF)	64
OSPF Areas	4 (3 areas plus area 0)
OSPF Adjacencies (devices per OSPF Area)	16
OSPF Link State Advertisements (LSA)	4,000
OSPF Virtual Links	4
ECMP (Max concurrent equal cost paths)	4
ECMP (Max next hop entries)	128
VRRP Instances	64
Management Routes	4
UDP Forwarding Entries	128
DHCP Relay Entries	256
DHCP Relay Forward Paths	512
Fabric Connect (SPB)	
SPB operational mode	Standalone or stack of up to 8 units
SPB nodes per region	450
SPB (IS-IS) adjacencies	4
SPB Customer VLANs (C-VLANs)	500
SPB I-SIDs	500
SPB Switched UNIs	500
Number of B-VLANs	2
Number of IS-IS interfaces	4
Number of Layer 2 VSNs that can be configured on switch	500 per stack ✱ **Note:** This includes 256 Layer 2 VSNs that can be configured for SPBM multicast (by enabling IGMP Snooping on them).

Table continues…

Feature	Maximum Number Supported in ERS 5900 series
Maximum number of different multicast streams supported (identified by source/group IP and ingress C-VLAN)	From 283 to 500 The following formula applies: $1024\ ENTRIES >= L2\_VSN + 2 \times MC\_STREAMS + 8$ (reserved) Where, • ENTRIES is the total number of entries supported. • L2_VSN is the number of L2_VSNs (with or without IGMP snooping). • MC_STREAMS is the number of IP Multicast streams, local + remote. For remote streams, two entries are occupied and for local streams, only one entry is occupied. ✱ **Note:** For each L2 VSN (C-VLAN or Switched-UNI) created on the SPBM device, an entry is occupied in a hardware table. For each multicast stream, two entries are occupied in the same table, one for the source and one for the receiver, on both the source and client BEBs. The total number of entries is 1,024, where eight entries are unavailable (used internally by the system). The multicast traffic will work only for the streams that occupied the necessary entries in the hardware table. For example, if there are 500 multicast streams in one C-VLAN, 1,001 hardware entries will be occupied: 500 for the source of the traffic, 500 for the receivers, and one for the C-VLAN.
Miscellaneous	
Maximum Admin Accounts	25
IGMP v1/v2 multicast groups	up to 1,024 (for 1,024 distinct streams) ✱ **Note:** These limits do not indicate that 1,024 entries are actually available because the installation of IP Multicast entries in hardware is also determined by the available free entries. One IP Multicast table is shared between multicast applications.
IGMP Enabled VLANs	256
Aggregation groups (link aggregation)	32

Table continues…

DRAFT—November 4, 2015—4:41 AM (UTC)

Feature	Maximum Number Supported in ERS 5900 series
Ports per aggregation group	8
802.1x (EAP) clients per port, running in MHMV	32
802.1x (NEAP) clients per switch/stack	384
802.1x (EAP & NEAP) clients per switch/stack	768
Maximum RADIUS Servers	2
Maximum 802.1X EAP Servers	2
Maximum 802.1X NEAP Servers	2
Maximum RADIUS/EAP/NEAP Servers	6
IPFIX number of sampled flows	100,000
LLDP Neighbors per port	16
LLDP Neighbors	800
RMON alarms	800
RMON events	800
RMON Ethernet statistics	110
RMON Ethernet history	249
Link State Tracking: Instances	2
Port Mirroring Instances	4 ✴ **Note:** Only three RSPAN instances can be created.
Port Mirroring: RSPAN VLANs	4
Port Mirroring: RSPAN destinations	4 per switch or stack
IPv6 DHCP relay forward paths	256
IPv6 static routes	512
IPv6 interfaces	256
IPv6 tunnels	4
PIM-SM multicast entries	Up to 1,024 The platform supports a maximum of 1,024 IPMC forwarding entries. These limitations are imposed on standalone ERS 59xx devices and stacks. ✴ **Note:** These limits do not indicate that 1,024 entries are actually available because the installation of IPMC entries in hardware is also determined by the available free entries.
Maximum PIM-SM interfaces	64 (4 active, 60 passive)

Table continues…

Feature	Maximum Number Supported in ERS 5900 series
Allow-flood IGMP multicast addresses	Allow-flood entries are programmed for a multicast MAC (except MAC ranges used by IPv4 and IPv6 multicast), an IPv4 multicast IP address or an IPv6 multicast IP address. An entry applies to a specified VLAN. Box-wide maximums are: • 128 multicast MAC entries • 128 IPv4 multicast IP entries • 128 IPv6 multicast IP entries Allow-flood for IPv4 addresses is not permitted on SPBM C-VLANs. A warning is issued if you attempt this configuration.

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 Static Routing

All other features in Release 7.0.1 are included with the base license.

You can obtain a trial license to try out advanced license features for 60 days. Trial licenses are obtained from Avaya and installed using the ACLI. 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 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 (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1X (EAPOL)
- IEEE 802.1ab (Link Layer Discovery Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)

RFCs

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

- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 951 (BootP)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)

1 • RFC 1271 (RMON)

2 • RFC 1350 (TFTP)

3 • RFC 1493 (Bridge MIB)

4 • RFC 1757 (RMON)

5 • RFC 1945 (HTTP v1.0)

6 • RFC 2131 (DHCP)

7 • RFC 2236 (IGMPv2)

8 • RFC 2362 (PIM-SM)

9 • RFC 2474 (QoS)

10 • RFC 2597 (QoS)

11 • RFC 2598 (QoS)

12 • RFC 2665 (Ethernet MIB)

13 • RFC 2674 (Q-BRIDGE-MIB)

14 • RFC 2737 (Entity MIBv2)

15 • RFC 2819 (RMON MIB)

16 • RFC 2863 (Interfaces Group MIB)

17 • RFC 2865 (RADIUS)

18 • RFC 3140 (QoS)

19 • RFC 3246 (QoS)

20 • RFC 3410 (SNMPv3)

21 • RFC 3411 (SNMP Frameworks)

22 • RFC 3412 (SNMP Message Processing)

23 • RFC 3413 (SNMPv3 Applications)

24 • RFC 3414 (SNMPv3 USM)

25 • RFC 3415 (SNMPv3 VACM)

26 • RFC 3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service)

27 The following table lists IPv6 specific RFCs.

Standard	Description	Compliance
RFC 1886	DNS Extensions to support IPv6	Supported
RFC 1981	Path MTU Discovery for IPv6	Supported
RFC 2460	Internet Protocol v6 (IPv6) Specification	Supported

Table continues…

Standard	Description	Compliance
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 4007	Scoped Address Architecture	Supported
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	Not 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 4301	Security Architecture for the Internet Protocol	Not supported
RFC 4443	Internet Control Message Protocol (ICMPv6)	Support earlier version of RFC (2463)

Chapter 4: Resolved issues

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

Reference Number	Description
wi01230478	ACLI command `snmp-server view` processes successive OID view specification arguments and the commands generated in the ASCII configuration files are applied correctly.
wi01217504	ADAC uplink-port configuration does not fail.
wi01223727	Fabric Attach time-out value can be seen and configured using EDM.
wi01223927	ACLI command `show interface` output displays all the interfaces.
wi01226191	After a reboot, the switch retains configurations such as, DHCP-Snooping, ARP-Inspection, IP Source Guard applied on a dynamic VLAN created by the FA agent.

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 and Limitations for Release 7.0.1

The following table lists known issues and limitations for Software Release 7.0.1.

Change Request number	Description
ERS495900-629 ERS495900-625	On Fabric Attach (FA) Server in Multiple Host Single Authentication (MHSA) mode, standard VLAN attribute is not processed for the authenticated client when multiple (VLAN:ISID) bindings are returned from RADIUS server. WORKAROUND: Standard VLAN must be changed to (VLAN:ISID) binding.
ERS495900-1079	On a stack running FA in FA Standalone Proxy mode, if a static uplink port (not a trunk) is configured and the port is not on the Base Unit, the configuration setting is lost when either the stack or only the Base Unit is reset. WORKAROUND: Utilize a static uplink trunk or a static uplink port on the Base Unit in a stack running FA in FA Standalone Proxy mode.

Known issues and limitations for Releases prior to 7.0.1

The following section lists known issues and limitations present in older releases of the software.

Table 4: Known issues from previous release

Change Request number	Description
wi01226049	When a Distributed Multiple Link Trunk (DMLT) is used as an SPB User to Network Interface (UNI), after a switch in stack with port member of the DMLT leave and rejoin the stack, broadcast and multicast traffic are not forwarded on the DMLT ports of that unit.

Table continues…

Change Request number	Description
	WORKAROUND: Force a link down and link up on the affected ports.
wi01187211	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.
wi01190566	When using certain browsers, the bar at the bottom of the page may automatically shift to the right when selecting a cell in the VLAN tab.
wi01198235	The L2 TraceMroute tab in EDM is empty. WORKAROUND: Use the ACLI command: **l2 tracemroute**.
wi01199982	The MAC addresses are learned even when MAC address learning is disabled and traffic enters through non-base unit (NBU) ports.
wi01202444	SLAMon tests are not supported on a switch configured with SPBM with NNI ports where the probes are sent over these types of ports. In addition, DSCP may be reset to zero over C-VLAN ports.
wi01203459	SPBM, Port Mirroring: When mirroring SPBM egress traffic, the mirrored traffic does not contain the MAC-in-MAC encapsulation or the 802.1ah header. The issue affects any kind of MAC-based mirroring.
wi01204174	When L3 is enabled on the device, the loopback port cannot be reserved for SPBM. WORKAROUND: Disable IP routing before enabling SPBM.
wi01206409	SNMP users cannot be created from the EDM Offbox. WORKAROUND: Create SNMP users from EDM or ACLI.
wi01207041	QoS Queue Stats cannot be cleared using EDM. WORKAROUND: Use ACLI command: **qos clear-queue-stats**.
wi01207480	After the password aging time expires, the user cannot change the password using EDM and connect to EDM. WORKAROUND: Use ACLI command **username password** to change the user's password.
wi01208072	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 5900 Series*, NN47211-502 for more information regarding MSTP.
wi01209290	QoS support over SPBM gives results different than expected. • Interface shaper shows lower rates than expected on traffic that enters UNI ports and exits NNI ports, also lower rates than expected on broadcast that enters NNI and exits UNI. • Meter shows lower rates than expected on traffic that enters NNI and exits UNI.

Table continues…

Change Request number	Description
	• Queue shaper shows lower rates than expected on unicast traffic that enters UNI and exits NNI. Some small floods/dropped traffic may be present. • IP-elements, actions and set-egress-non-unicast do not work on traffic that enters NNI and exits UNI.
wi01209636	SPBM Multicast: Multicast stream is not removed when access ports are disabled. Multicast streams will be aged out.
wi01210784, wi01218663	EDM: The values for Clear Time and Clear Counter is not displayed correctly. Navigate to path **Configuration > Serviceability > IPFIX > Collectors > Graph** and verify **Exporter** tab and **Clear Time** tab. The value for Clear Time is displayed as 0day, 00h:00m:00s and Clear Counters does not work for AbsoluteValue.
wi01213020	In a certain scenario when a non-SPBM device is connected to a BEB, the multicast traffic is sent over the primary B-VLAN only. The limitation only applies when multicast traffic is local to the switch stack (UNI ports) and there are local (UNI side) membership reports on DMLTs (remote streams or remote members are still supported).
wi01213087	Cable diagnosis is not performed for multiple ports on different units.
wi01216173	SPBM, Port Mirroring: With SPBM Multicast enabled, if you mirror a port with IS-IS enabled, multicast streams that ingress on the local stack and egress on the mirror port will have the MAC-in-MAC 802.1ah header stripped and the customer VLAN ID replaced with 0xFFF (4095).
wi01218663	Cannot clear the stats from SNMP for a collector configured when using rcIpfixExporterStatsClear MIB object. WORKAROUND: Use ACLI.
wi01219325	The information displayed in the Interface SPBM tab in EDM is doubled. The ACLI command works as expected.
wi01219332	Using l2 ping from the EDM offbox does not work. WORKAROUND: Use the ACLI **l2 ping** command.
wi01220242	Message indicating the SPBM reserved ports are 'bad port numbers' is misleading. The error message should state these ports are unavailable for general use.
wi01220686	DHCP Snooping binding table is not populated in an SPBM environment where DHCP server and DHCP client are connected to different C-VLANs with the same I-SID (DHCP server is reached over SPBM cloud). To avoid this issue, configure the same VLAN I-SID on both server and client.
wi01220839	After a base unit reset, NEAP clients connected to non-base units in a stack may not be re-authenticated if QoS UBP Support Level is High Security Local Data. WORKAROUND: After the NEAP clients are cleared and authenticated to the RADIUS server, re-authentication functions as expected.
wi01220991	Non-unicast traffic hashing over MLT: The non-unicast traffic hashing formula using the destination IP as a parameter does not issue an error message when the destination IP is not a multicast IP.

Table continues…

Change Request number	Description
wi01221033	Changing the RADIUS user password is not working when out-of-band management IP is in use.
wi01221098	When creating AES schedules one minute after another (activate and deactivate), the last settings are lost (only activate is configured). When creating another deactivate schedule one minute before the activate schedule, the settings are overwritten and both deactivates are written.
wi01222023	User should be prevented from assigning an I-SID to an RSPAN VLAN.
wi01222045	Telnet session is disconnected when IP routing is disabled from an EDM console session.
wi01222188	When issuing a **show ip** command from a non-base unit console on a stack running in TBU mode, the Default Gateway is not displayed as 'In Use'. This is a display issue only.
wi01222303	User is unable to reserve SPBM port while unknown-mcast-no-flood is enabled.

WORKAROUND: Disable unknown-mcast-no-flood before enabling SPBM. |
| wi01222331 | SLAMon NTR test is not working from EDM.

WORKAROUND: Use ACLI command **slamon ntr**. |
| wi01222464 | 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. |
| wi01222483 | If an entry fails to be created in ntnQosIfShapingTable, the index used in the failed request is no longer available. |
| wi01222640 | When mapping a VLAN to a non-existent STG using EDM, the error message displays an incorrect STG number. |
| wi01222711 | 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.

WORKAROUNDS:

1. Increase the timeout and retries for the RADIUS server (for example, 5 retries and 10 second timeout).

2. Use Fail Open VLAN to address the RADIUS connectivity issues.

3. Enable reauthentication. |
| wi01222747 | Configuring non-default community strings using the Quick Start in EDM does not work.

WORKAROUND: Configure the community strings in EDM under **Configuration > Edit > Snmp Server > Community** or in ACLI. |
| wi01222880 | Cable diagnosis is not performed for multiple ports on different units.

WORKAROUND: Use the ACLI command from the unit for which you want to perform TDR. |

Table continues…

Change Request number	Description
wi01223102	In ACLI, in the quick install script, when entering an invalid VLAN identifier for the Quick Start VLAN, the error message changes if you try to reenter an invalid value.
wi01223151	The help for the ACLI command **no ipv6 mgmt interface process-redirect** command reads 'Enable processing IPv6 redirect-msg' when it should read 'Disable processing IPv6 redirect-msg'.
wi01223154	EDM: IPv6 default gateway cannot be configured from EDM. WORKAROUND: Use ACLI to configure the default gateway.
wi01223243	There is an inconsistency between the range of values allowed for the **ipv6 nd hop-limit** CLI setting (1-255) and the range allowed when setting the Ipv6RouterAdvertCurHopLimit MIB object (0-255). A value of zero in the router advertisement indicates the advertisement isn't specifying a value for curHopLimit and can only be set via SNMP or in EDM.
wi01223263	In the scenario where the STP mode has been changed and the stack rebooted, the ACLI command **show ipv6 mld interface** issued immediately after the stack has been formed results in the following error message: '% NULL error pointer'.
wi01223298	SPBM MHMV: NEAP client is not removed from NEAP authenticated list when the ACLI command **clear mac-address-table address <address>** is used on NBU ports. WORKAROUND: Use one of the following ACLI commands: **clear eapol non-eap address <address>**, **clear mac-address-table interface Ethernet <port_list>**, or a general **clear mac-address-table**.
wi01223348	In MHSA mode, if the EAP client has no valid RADIUS Assigned VLAN configured on the RADIUS server, the port priority will not be displayed in ACLI.
wi01223354	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**.
wi01223623	If your system is configured with the maximum number of Voice VLANs (6), using EDM to create additional VLANs results in an error message 'Maximum number of Voice VLANs reached' even if the newly added VLAN does not have the VoiceEnabled option selected. WORKAROUND: Use the **vlan create** ACLI command to create new VLANs.
wi01223662	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.
wi01223751	Link State Tracking: bsLstGroupOperStateChanged traps are not generated when the last upstream interface goes up or down. The events are recorded in the System Log.
wi01223755	An incorrect error message appears when an IPv4 interface is created after 256 IPv6 interfaces have already been added.

Table continues…

Change Request number	Description
wi01223817	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.
wi01223891	When performing an SNMP Get/Get Next/Walk operation on the etherStatsOwner MIB object or etherStatsTable MIB table, for RMON statistics which do not have an owner configured, an output which contains unexpected characters may be obtained for the owner string instead of no value.
wi01223929	When trying to restore the DHCP Snooping binding table and no DHCP Snooping external device is configured , '% Commit failed' message will be displayed.
wi01223987	IPFIX table will not show IP flow information if the observation port is set on NNI interface on an SPBM enabled interface.
wi01224032	When displaying port mirroring in EDM, port number 128 is displayed for mirror ports that are not used.
wi01224130	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.
wi01224135	If mac-max is changed to a higher value while EAP and NEAP clients are authenticated on the same port, the NEAP clients are lost and do not reauthenticate. WORKAROUND: Disable and enable EAP globally to reauthenticate EAP/NEAP clients.
wi01224162	Autotopology: 0.0.0.0 entry is not displayed in the autotopology table when the device does not have the IP address.
wi01224293	EDM Help: When you select Help for the Fabric Attach Agent tab, the information is incomplete and incorrectly refers to the Agent tab as the SPBM tab.
wi01224296	Critical logs associated with exceptions are not sent to remote system log.
wi01224319	The ACLI command **lldp tx-tlv dot1 protocol-identity EAP LLDP STP** only applies the first protocol identity specified. WORKAROUND: Specify each protocol identity in a separate ACLI command.
wi01224441	SPBM Multicast: no error message is generated if SPBM Multicast is enabled when all precedences on all ports are occupied. The ERS 5900 has a total of 16 precedences available. Applications including DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, SPB, QoS, and EAP use these precedences. Use the ACLI command **show qos diag** to display the current use of precedence resources.
wi01224917	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.

Table continues…

Release Notes for Avaya ERS 5900
DRAFT—November 4, 2015—4:41 AM (UTC)

Change Request number	Description
	WORKAROUND: Use the serial console on the temporary base unit or use telnet/SSH to view the correct QoS UBP statistics.
wi01224979	STPG multicast MAC address cannot be configured from EDM. WORKAROUND: Use the **spanning-tree multicast** ACLI command.

Limitations and considerations

The following table lists known limitations and considerations:

Table 5: Ethernet Routing Switch 5900 Series considerations

Item	Description
1	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.
2	Avoid using MAC security on a trunk (MLT).
3	Failed attempts to log in (using TACACS+ authentication and accounting) are not stored in the accounting file.
4	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	When you use the EDM/Web to configure and add VLAN ports to an STG other than the default STG, STG membership of the port may change. In that case, the new STG participation of that port will be disabled. WORKAROUND: Enable participation of the ports in the new STG after you enable the STG.
6	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).
7	The IPFIX sampling data rate cannot be changed because of a related hardware limitation.
8	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.

Table continues…

Item	Description
	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.
9	Do not enable IP Source Guard on trunk ports.
10	Non-existent VLAN Mapping for MSTI: EDM/SNMP support for VLAN Mapping for MSTI is not available.

11	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.`

12	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
13	In a stack configuration, SSHC configuration options are only available from the base unit

14	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`

15	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

Table continues…

Item	Description
	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.
16	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.
17	SPBM, Port Mirroring: With SPBM Multicast enabled, if you mirror a port with IS-IS enabled, multicast streams that ingress on the local stack and egress on the mirror port will have the MAC-in-MAC 802.1ah header stripped and the customer VLAN ID replaced with 0xFFF (4095).
18	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`
19	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).

VLACP issue

In some situations, when you use VLACP the ERS 5900 series 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 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.

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

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

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

Table 6: Application mask and filter resource requirements

Application	Category	Masks required	Filters required
Ethernet Routing Switch 5900 Series			
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)	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]
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]

Table continues…

Application	Category	Masks required	Filters required
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 ERS 5900 Series switches 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 and two filters per port for ARP filtering, and one mask and two filters per port for DHCP relay. This leaves 14 masks available, each with 254 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 ERS 5900 Series 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 ERS 5900 Series switches, 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.

Example - IP Source Guard on an ERS 5900 Series switch port

On ERS 5900 Series switches 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).

✱ **Note:**

The switch supports only full-duplex operation.

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
```