Release Notes for Avaya Ethernet Routing Switch 4000 Series

Release 5.7.3
NN47205-400
Issue 11.01
November 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

License types

Heritage Nortel Software

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

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

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

Licence types

Heritage Nortel Software

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

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

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

Contents

Chapter 1: Introduction

Purpose

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

The following switch models are supported:

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

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

Related resources

Documentation

For a list of the documentation for this product and more information about documents on how to configure other switch features, see *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101.

For more information on new features of the switch and important information about the latest release, see *Release Notes for Avaya Ethernet Routing Switch 4000 Series*, NN47205-400.

For more information about how to configure security, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

For the current documentation, see the Avaya Support web site: www.avaya.com/support.

Training

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

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

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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

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

Note:

Videos are not available for all products.

Searching a documentation collection

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

Before you begin

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

Procedure

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

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

Subscribing to e-notifications

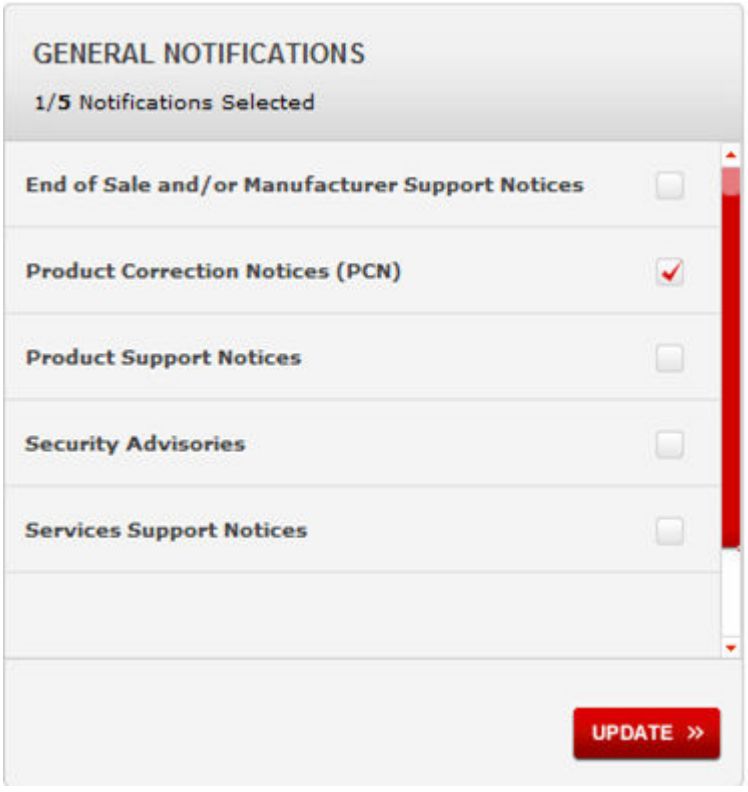
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

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

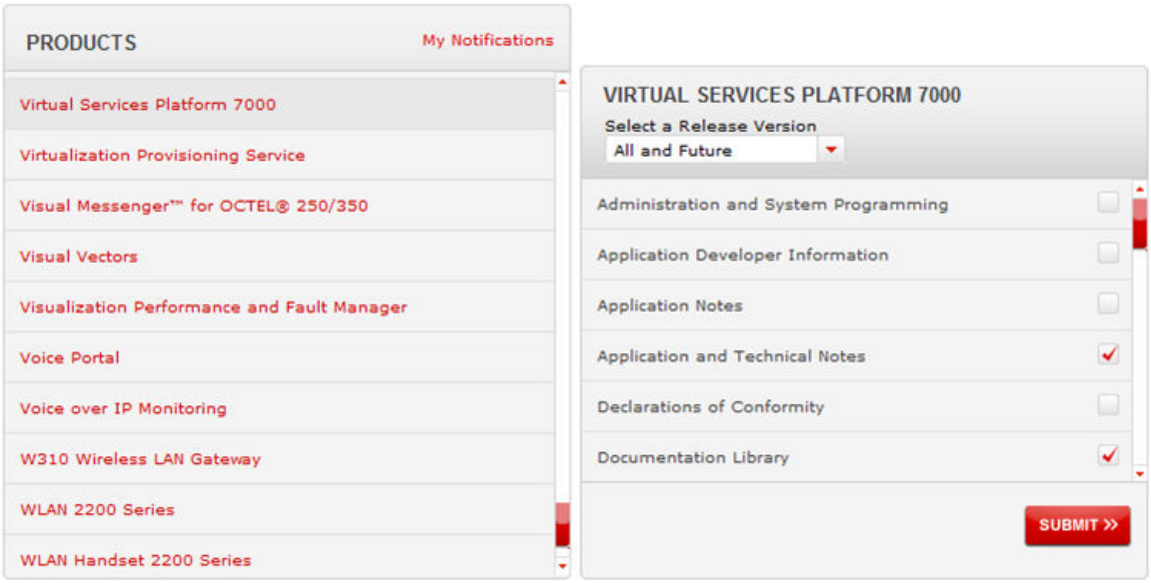
Procedure

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



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

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



11. Click **Submit**.

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 *Avaya Ethernet Routing Switch 4000 Series Release Notes* — Software Release 5.7.3.

Features for Release 5.7.3

See the following sections for information about the new features for Release 5.7.3.

Removal of SPB support for ERS 4000

In Release 5.7.3, the Shortest Path Bridging (SPB) functionality is no longer supported for ERS 4000 switches in order to support the integration of Fabric Attach functionality.

Note:

For ERS 4800 customers wishing to deploy both SPB and Fabric Attach features, Avaya recommends upgrading to Release 5.9.x of ERS 4000 software.

Booting with an ASCII configuration file from the local file system

This feature allows you to download an ASCII configuration file from a TFTP server or USB to the local file system and boot the system with the local ASCII configuration file. Two ASCII configuration files are supported, one in each block.When you download and save an ASCII configuration file to the local file system, the system deletes the old file in that block.

For ERS 4500, the maximum size of an ASCII configuration file is limited to 150 kilobytes.

This feature introduces the following ACLI commands:

- show script block
- copy tftp script
- copy usb script
- boot nvram block
- boot script block

For more information, see Booting with an ASCII configuration file on page 46.

Fabric Attach

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

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

The Fabric Attach support is limited to the Fabric Attach proxy function. Fabric Attach server and client operations are not supported.

ACLI commands

This feature introduces the following ACLI commands:

- fa authentication-key
- default fa authentication-key
- extended-logging
- no extended-logging
- fa message-authentication
- default fa message-authentication
- no fa message-authentication
- fa port-enable
- default fa port-enable
- no fa port-enable
- fa proxy
- default fa proxy
- no fa proxy
- fa standalone-proxy
- fa timeout
- default fa timeout
- fa uplink
- fa uplink port
- fa uplink trunk
- fa vlan
- no fa vlan
- fa zero-touch

- fa zero-touch
- no fa zero-touch
- default fa zero-touch
- fa zero-touch-options
- fa zero-touch-options
- no fa zero-touch-options
- default fa zero-touch-options
- show fa agent
- show fa elements
- show fa i-sid
- show fa assignment
- show fa port-enable
- show fa interface
- show fa uplink
- show fa vlan
- show fa zero-touch-options

For more information about the Fabric Attach feature, see *Configuring Avaya Fabric Attach on Avaya Ethernet Routing Switch 4000 Series*, NN47205-508.

Chapter 3: Important notices

The following sections provide important notices.

Supported software and hardware capabilities

The following table lists supported software and hardware scaling capabilities in Avaya Ethernet Routing Switch 4000 Series Software Release 5.7. The information in this table supersedes information contained in any other document in the suite.

Table 1: Supported software and hardware scaling capabilities

Feature	Maximum number supported
Egress queues	Configurable 1–8
MAC addresses	8,192
Stacking bandwidth (full stack of 8 units)	Up to 384 Gbps
QoS precedence	8 per ASIC
QoS rules per ASIC	128 rules per precedence
Maximum number of units in a stack	8
Maximum number of Port Mirroring Instances	4
Layer 2	
Concurrent VLANs	1,024
Supported VLAN IDs	1 - 4094 (0 and 4095 reserved; 4001 reserved by STP; 4002-4008 reserved by multiple STP groups)
Protocol VLAN types	7
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32
Maximum MAC Learning rate on an MLT trunk	500 new MAC addresses per second
Links or ports for MLT, DMLT or LAG	8
Static MAC Addresses	1,024
Spanning Tree Group instances (802.1s)	8

Table continues…

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

Table continues…

Feature	Maximum number supported
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
Port Mirroring: RSPAN VLANs	4
Port Mirroring: RSPAN destinations	4 per switch or stack

Filter, meter and counter resources

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

Note:

Filters will use the highest available precedence.

Table 2: Filter, meter and counter resources per port

Feature	Observation	QoS			NonQos	
		Filters	Meters	Counter	Filters	Meters
EAPOL		0	0	0	2	0
ADAC		0	0	0	1	0
DHCP Relay	L2 mode	0	0	0	0	0
DHCP Relay	L3 mode	0	0	0	0	0
DHCP Snooping		0	0	0	2	1
MAC Security		0	0	0	0	0
IP Source Guard		0	0	1	11	0
Port Mirroring	Mode XrxYtx	1	0	0	0	0
Port Mirroring	XrxYtx or YrxXtx	0	0	0	2	0
Port Mirroring	AsrcBdst, Asrc, Adst	1	0	0	0	0
Port Mirroring	AsrcBdst or BscrAdst, Asrc or Adst	2	0	0	0	0

Table continues…

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

File names for this release

File names for release 5.7.3

The following table describes the Avaya Ethernet Routing Switch 4000 Series, Software Release 5.7.2 software files. File sizes are approximate.

Table 3: Software Release 5.7.3 components

Module or File Type	Description	File Name	File Size (bytes)
Standard Runtime Software Image	Standard image for the Avaya Ethernet Routing Switch 4000 Series	4000_573030.img	9,691,280
Secure Runtime Software Image	Secure image for the Avaya Ethernet Routing Switch 4000 Series	4000_573031s.img	9,953,984
Diagnostic Software Image	4500 diagnostic image (except 4500–PWR+ models)	4500_53003_diag.bin	1,589,514
	4000 diagnostic image (4500–PWR+ and 4800 models)	4000_57001_diag.bin	1,934,097
	4000 combination diagnostic image (all 17 models)	4000_57001_combodiag.bin	3,523,611
PoE Firmware	PoE Firmware for ERS 4500 (4526T-PWR, 4550T-PWR, 4524GT-PWR, 4526GTX-	4500_PoE_400.img	77,766

Table continues…

Module or File Type	Description	File Name	File Size (bytes)
	PWR, 4548GT-PWR with 'Nortel' logo)		
	PoE Firmware for ERS 4500-PWR (4526T-PWR, 4550T-PWR, 4524GT-PWR, 4526GTX-PWR, 4548GT-PWR HW with 'Avaya' logo	4500_PoE_400b15.img	77,923
	Note: From Release 5.6.2, when the firmware image is provided, the software detects and matches the correct firmware with the hardware. For example, enter 4500_PoE_400.img and then, enter 4500_PoE_400b15.img, the correct firmware is matched with the hardware.		
PoE+ Firmware	PoE+ Firmware for 4526T-PWR+, 4550T-PWR+, 4826GTS-PWR+, 4850GTS-PWR+	4000_PoEplus_410B4.bin	16,384
Bootloader **Note:** The bootloader software is listed for completeness and is factory installed on new revision 10 hardware, there is no requirement to update the bootloader.	Bootloader image for 4500-PWR+ and 4800 models	4000_56108_boot.bin	322,522
Enterprise Device Manager Help Files	Help files required for Avaya Ethernet Routing Switch 4000	ers4500v573_HELP_EDM.zip	3,406,615
Enterprise Device Manager Plug-in	Avaya Ethernet Routing Switch 4000 Enterprise Device Manager plug-in for Configuration and Orchestration Manager	ers4000v5.7.3.0.zip	4,850,940
Software Release 5.7 Management Information Base (MIB) Definition Files	MIB definition files	Ethernet_Routing_Switch_4000_MIBs_5.7.3.zip	2,334,463

Supported traps and notifications

For information about SNMP traps generated by the Avaya Ethernet Routing Switch 4000 Series, see .

Supported Web browsers for Enterprise Device Manager

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

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

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

Upgrading software

To upgrade to the new software release 5.7, Avaya recommends that you first verify or upgrade the diagnostics image. For ERS 4500 models (excluding the 4526T-PWR+ and 4550T-PWR+), you are recommended to use version 5.3.0.3 of the diagnostics. For all 4800, as well as the 4526T-PWR+ and 4550T-PWR+ models, use the 5.7.0.1 diagnostics. Once the diagnostics image is verified or updated, you can then upgrade the agent version to release 5.7.3.

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

The following table describes possible image locations:

Table 4: Possible scenarios

Image	Location
Local Agent Image	Agent image in the flash memory of the unit.
Local Diagnostic Image	Diagnostic image in the flash memory of the unit
5.1.0.7 Diagnostic Image	Diagnostic image released in 5.1
5.2.0.3 Diagnostic Image	Diagnostic image released in 5.2
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.3
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.4
5.3.0.3 Diagnostic Image	Diagnostic image released in 5.5
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX,	Diagnostic image released in 5.6

Table continues…

Image	Location
4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	
5.6.0.15 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6
Combo 5.6.0.15 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.0.15 and can be downloaded on all units	Diagnostic image released in 5.6
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.6.1
5.6.1.18 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.1
Combo 5.6.1.18 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.1.18 and can be downloaded on all units	Diagnostic image released in 5.6.1
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.6.2
5.6.2.01 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.2
Combo 5.6.2.01 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.2.01 and can be downloaded on all units	Diagnostic image released in 5.6.2
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.6.3
5.6.2.01 Diagnostic Image for the following units: 4550T-PWR+, 4526T-PWR+, 4850GTS, 4850GTS-PWR+, 4826GTS, 4826GTS-PWR+	Diagnostic image released in 5.6.3
Combo 5.6.2.01 Diagnostic Image that is a combination between 5.3.0.3 and 5.6.2.01 and can be downloaded on all units	Diagnostic image released in 5.6.3
5.3.0.3 Diagnostic Image for the following units: 4524GT, 4524GT-PWR, 4526FX, 4526GTX, 4526GTX –PWR, 4526T, 4526T-PWR, 4548GT, 4548GT-PWR, 4550T, 4550T-PWR	Diagnostic image released in 5.7

Table continues…

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

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

Important:

You can upgrade any previous release software to the 5.7.3 Agent image. For the six new models introduced in Release 5.6, you must use the 5.6.0 Agent image as the minimum supported software revision either standalone or if the unit is stacked with any other ERS 4000 models.

Important:

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

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

When loading software release 5.7.3 it is mandatory that the switches are loaded with either 5.3.0.3 and/or 5.7.0.1 or later diagnostic software due to the increased size of the runtime agent code.

Use the following procedure to upgrade the Agent Image from release 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7.0, 5.7.1, or 5.7.2 to release 5.7.3:

Upgrading Agent Image from release 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7.0, 5.7.1, or 5.7.2 to release 5.7

1. Upgrade the diagnostic image from the earlier release to release 5.3.0.3 diagnostic image and/or 5.7.0.1 diagnostic image.
2. Upgrade the agent image from release 5.0, 5.1, 5.2, , 5.3, 5.4, 5.5, 5.6, 5.7.0, 5.7.1, or 5.7.2 to release agent image 5.7.3.

Warning:

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

Effects of Upgrade on Unified Authentication

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

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

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

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

The following message appears in system log :

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

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

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

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

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

With the unified authentication approach, when configuring RADIUS or TACACS+ on a stack, the authentication type is also applied to each switch within the stack. Consideration needs to be given for removal of a switch from the stack if a standalone switch IP address is not configured. If a switch within a stack does not have a standalone Switch IP address configured, then when either RADIUS or TACACS+ authentication is configured for the stack, this authentication method will not be applied to the respective standalone switch authentication and will only be applied to the stack and

any switches with standalone IP addresses. The following log message appears in System log when such a configuration is made in stack:

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

Effects of Upgrade on SNMP Trap Notifications

Important:

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

You can use the following procedures to restore trap functionality.

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

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

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

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

To reconfigure traps, use the following EDM procedure:

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

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

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

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

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

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

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

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

Table continues…

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Updating switch software

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

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

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

OR

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

See the following sections for details about updating switch software:

- General software upgrade instructions on page 27

- Changing switch software in ACLI on page 27
- Changing switch software in EDM on page 29

General software upgrade instructions

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

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

Changing switch software in ACLI

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

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

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

3. Press `Enter`.

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

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

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

Important:

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

Job aid—download command parameters

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

Table 5: ACLI download command parameters

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

Table continues…

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

Changing switch software in EDM

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

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

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

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

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

Important:

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

Job aid—File System screen fields

The following table describes the File System screen fields.

Table 6: File System screen fields

Field	Description
TftpServerInetAddress	Indicates the IP address of the TFTP or SFTP* server on which the new software images are stored for download.
TftpServerInetAddressType	Indicates the type of TFTP or SFTP* server address type: • IPv4 • IPv6
BinaryConfigFileName	Indicates the binary configuration file currently associated with the switch. Use this field when you work with configuration files; do not use this field when you download a software image.
BinaryConfigUnitNumber	When in standalone mode, and loading a binary configuration file that was created from a stack, this object specifies the unit number of the portion of the configuration file to be extracted and used for the standalone unit configuration. If this value is 0, it is ignored.
ImageFileName	Indicates the name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.
FwFileName (Diagnostics)	The name of the diagnostic file currently associated with the switch. If needed, change this field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	Indicates the unit number of the USB port to be used to upload or download a file. A value of 0 indicates download is via TFTP; a value of 9 indicates a standalone switch and a value of 10 indicates SFTP* server.
Action	This group of options represents the actions taken during this file system operation. The options applicable to a software download are • dnldConfig: Download a configuration to the switch. • dnldConfigFromSftp: Download a configuration to switch from the SFTP Server*. • dnldConfigFromUsb: Download a configuration to switch using the front panel USB port. • dnldFw: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwFromSftp: Download a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image*. • dnldFwFromSftpNoReset: Download a new diagnostic software image to the switch from the SFTP server. This

Table continues…

Field	Description
	option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset*. • dnldFwFromUsb: Download a new diagnostic software image to the switch from the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwNoReset: Download a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • dnldImg: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. • dnldImgFromSftp: Download a new software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image*. • dnldImgFromSftpNoReset: Download a new software image to the switch from the SFTP server. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset*. • dnldImgFromUsb: Download a new software image to the switch using the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. • dnldImgIfNewer: Download a new software image to the switch only if it is newer than the one currently in use. • dnldImgNoReset: Download a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • upldConfig: Upload a configuration to the switch from a designated location. • upldConfigToSftp: Upload binary config to SFTP server*. • upldConfigToUsb: Upload binary config to USB port • upldImgToUsb: Upload image to USB port

Table continues…

Field	Description
Status	Display the status of the last action that occurred since the switch last booted. The values that are displayed are • other: No action occurred since the last boot. • inProgress: The selected operation is in progress. • success: The selected operation succeeded. • fail: The selected operation failed.

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

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

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

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

The following table describes the ip.cfg file parameters:

Table 7: ip.cfg file optional parameters

Parameter	Description
IP <*xx.xx.xx.xx*>	Specifies the IP address for the switch. Example: 192.168.22.1
Mask <*xx.xx.xx.xx*>	Specifies the network mask. Example: 255.255.255.0
Gateway <*xx.xx.xx.xx*>	Specifies the default gateway. Example: 181.30.30.254
SNMPread <*string*>	Specifies the SNMP read community string. Example: public
SNMPwrite <*string*>	Specifies the SNMP write community string. Example: private
VLAN <*number*>	Specifies the management VLAN-ID. Example: VLAN 1
USBdiag <*string*>	Specifies the file name of the diagnostic image to load from the USB device. Example: ers4000/4000_5.3.0.34.bin
USBascii <*string*>	Specifies the file name of the ASCII configuration file to load from the USB device. Example: customer1.cfg

Table continues…

Parameter	Description
USBagent <*string*>	Specifies the file name of the runtime agent image to load from the USB device. Example: ers4000/4000_563024.img
NEXTIP, NEXTMask, and NEXTGateway	Specifies IP addresses, network mask and gateway to be used once the switch is rebooted.

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

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

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

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

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

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

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

Important:

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

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

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

1. Press `CTRL` and `y` keys together.

Two possible responses indicate a pass or fail status.

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

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

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

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

Hardware and software compatibility

This section provides hardware and software compatibility information.

XFP, SFP and SFP+ Transceiver Compatibility

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

Table 8: XFP and SFP transceiver compatibility

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

Table continues…

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
1000BASE-CWDM SFP	1550 nm LC connector, up to 40 km	5.0.0	AA1419029-E5
1000BASE-CWDM SFP	1570 nm LC connector, up to 40 km	5.0.0	AA1419030-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 40 km	5.0.0	AA1419031-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 40 km	5.0.0	AA1419032-E5
1000BASE-CWDM SFP	1470 nm LC connector, up to 70 km	5.0.0	AA1419033-E5
1000BASE-CWDM SFP	1490 nm LC connector, up to 70 km	5.0.0	AA1419034-E5
1000BASE-CWDM SFP	1510 nm LC connector, up to 70 km	5.0.0	AA1419035-E5
1000BASE-CWDM SFP	1530 nm LC connector, up to 70 km	5.0.0	AA1419036-E5
1000BASE-CWDM SFP	1550 nm LC connector, up to 70 km	5.0.0	AA1419037-E5
1000BASE-CWDM SFP	1570 nm LC connector, up to 70 km	5.0.0	AA1419038-E5
1000BASE-CWDM SFP	1590 nm LC connector, up to 70 km	5.0.0	AA1419039-E5
1000BASE-CWDM SFP	1610 nm LC connector, up to 70 km	5.0.0	AA1419040-E5
1000BSE-T SFP	Category 5 copper unshielded twisted pair (UTP), RJ-45 connector	5.0.0	AA1419043-E5
1000BASE-SX DDI SFP	850 nm DDI LC connector	5.2.0	AA1419048-E6
1000BASE-LX DDI SFP	1310 nm DDI LC connector	5.2.0	AA1419049-E6
1000BaseXD DDI SFP	1310nm LC connector	5.4.0	AA1419050-E6
1000BaseXD DDI SFP	1550nm LC connector	5.4.0	AA1419051-E6
1000BaseZX DDI SFP	1550nm LC connector	5.4.0	AA1419052-E6
1000BaseCWDM SFP	1470nm LC connector, up to 40km	5.4.0	AA1419053-E6
1000BaseCWDM DDI SFP	1490nm LC connector, up to 40km	5.4.0	AA1419054-E6
1000BaseCWDM DDI SFP	1510nm LC connector, up to 40km	5.4.0	AA1419055-E6

Table continues…

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
1000BaseCWDM DDI SFP	1530nm LC connector, up to 40km	5.4.0	AA1419056-E6
1000BaseCWDM DDI SFP	1570nm LC connector, up to 40km	5.4.0	AA1419058-E6
1000BaseCWDM DDI SFP	1590nm LC connector, up to 40km	5.4.0	AA1419059-E6
1000BaseCWDM DDI SFP	1610nm LC connector, up to 40km	5.4.0	AA1419060-E6
1000BaseCWDM DDI SFP	1470nm LC connector, up to 70km	5.4.0	AA1419061-E6
1000BaseCWDM DDI SFP	1490nm LC connector, up to 70km	5.4.0	AA1419062-E6
1000BaseCWDM DDI SFP	1510nm LC connector, up to 70km	5.4.0	AA1419063-E6
1000BaseCWDM DDI SFP	1530nm LC connector, up to 70km	5.4.0	AA1419064-E6
1000BaseCWDM DDI SFP	1550nm LC connector, up to 70km	5.4.0	AA1419065-E6
1000BaseCWDM DDI SFP	1570nm LC connector, up to 70km	5.4.0	AA1419066-E6
1000BaseCWDM DDI SFP	1590nm LC connector, up to 70km	5.4.0	AA1419067-E6
1000BaseCWDM DDI SFP	1610nm LC connector, up to 70km	5.4.0	AA1419068-E6
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC (Must be paired with AA1419070-E5)	5.2.0	AA1419069-E5
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC (Must be paired with AA1419069-E5)	5.2.0	AA1419070-E5
1000Base DDI SFP	1550nm LC connector, 120 km	5.4.0	AA1419071-E6
100BASE-FX SFP	1310 nm LC connector	5.0.0	AA1419074-E6
100BASE-BX SFP	100Base-BX10-U SFP Bidirectional upstream 1310nm TX 10km SFP (Must be deployed with AA1419083-E6 or similar 100Base-BX).	5.6.0	AA1419082-E6

Table continues…

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
100BASE-BX SFP	100Base-BX10-D SFP Bidirectional upstream 1530nm TX 10km (Must be deployed with AA1419082-E6 or similar 100Base-BX).	5.6.0	AA1419083-E6
100BASE-ZX SFP	100Base-ZX, 1550nm 70-80km SFP	5.6.0	AA1419084-E6
T1 SFP	1.544 Mbps Fast Ethernet to T1 remote bridge, RJ-48C	5.1.0	AA1419075-E6
1000BASE-BX SFP	1310nm LC connector, up to 40km (Must be paired with AA1419077-E6)	5.3.0	AA1419076-E6
1000BASE-BX SFP	1490nm LC connector, up to 40km (Must be paired with AA1419076-E6)	5.3.0	AA1419077-E6
10 Gigabit Ethernet XFP Transceivers			
10GBASE-LR/LW XFP	1-port 1310 nm SMF, LC connector	5.2.0	AA1403001-E5
10GBASE-SR XFP	1-port 850 nm MMF, LC connector	5.1.0	AA1403005-E5
10GBASE-ZR/ZW XFP	1550 nm SMF LC connector	5.1.0	AA1403006-E5
10GBASE-LRM XFP	1310 nm, up to 220 m over MMF, DDI	5.2.0	AA1403007-E6
10 Gigabit Ethernet SFP+ Transceivers			
10GBASE-LR SFP+	1–Port 10 Gigabit-LR SFP + (LC) Single mode up to 10 km	5.6.0	AA1403011–E6
10GBASE-ER SFP+	1–Port 10 Gigabit-ER SFP + (LC) Single mode up to 40 km	5.6.0	AA1403013–E6
10GBASE-SR SFP+	1–Port 10 Gigabit-SR SFP + (LC) Multi-mode fibre up to 300 m	5.6.0	AA1403015–E6
10GBASE-LRM SFP+	1–Port 10 Gigabit-LRM SFP+ (LC) Multi-mode fibre up to 220 m	5.6.0	AA1403017–E6
10GDAC-10M SFP+	SFP+ direct attach cable 10 m	5.6.0	AA1403018–E6

Table continues…

Supported XFPs, SFPs and SFP+s	Description	Minimum software version	Part Number
10GDAC-3M SFP+	SFP+ direct attach cable 3 m	5.6.0	AA1403019–E6
10GDAC-5M SFP+	SFP+ direct attach cable 5 m	5.6.0	AA1403020–E6

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

Supported standards, RFCs and MIBs

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

Standards

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

- IEEE 802.1 (Port VLAN, Port & Protocol VLANs, VLAN Name, Protocol Entity)
- IEEE 802.1AB (Link Layer Discovery Protocol)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1s (Multiple Spanning Trees)
- IEEE 802.1v (VLAN Classification by Protocol and Port)
- IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)
- IEEE 802.1X (EAPOL)
- 802.1X-2004 (Port Based Network Access Control)
- IEEE 802.3 (Ethernet)
- IEEE 802.3ab (1000BASE-T)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3ae (10Gb/s Ethernet)
- IEEE 802.3ae (10GBASE-LR/SR/LM)
- IEEE 802.3af (Power over Ethernet)

- IEEE 802.3at (Power over Ethernet)
- IEEE 802.3u (100BASE-FX)
- IEEE 802.3u (100BASE-TX)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (1000BASE-SX)
- IEEE 802.3z (1000BASE-x)
- IEEE 802.3z (Gigabit Ethernet over Fiber-Optic)
- IEEE P802.3ak (10GBASE-CX4)

RFCs and MIBs

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

- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 951 (BootP)
- RFC 1058 (RIP v1)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)
- RFC 1271 (RMON)
- RFC 1305 (Network Time Protocol Version 3)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 1583 (OSPF v2)
- RFC 1757 (RMON)
- RFC 1850 (OSPF v2 MIB)

- RFC 1945 (HTTP v1.0)
- RFC 2131 (BootP/DHCP Relay Agent)
- RFC 2236 (IGMPv2)
- RFC 2328 (OSPF v2)
- RFC 2453 (RIP v2)
- RFC 2474 (Diffserv)
- RFC 2475 (Diffserv)
- RFC 2665 (Ethernet MIB)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 2715 (Interoperability Rules for Multicast Routing Protocols)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2865 (RADIUS)
- RFC 2866 (RADIUS Accounting)
- RFC 2933 (Internet Group Management Protocol MIB)
- RFC 3046 (DHCP Relay Agent Information Option)
- RFC 3246 (Expedited Forwarding Behavior)
- RFC 3376 (Internet Group Management Protocol, Version 3)
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)
- RFC 3412 (SNMP Message Processing)
- RFC 3413 (SNMPv3 Applications)
- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3569 (An Overview of Source-Specific Multicast [SSM])
- RFC 3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service [RADIUS])
- RFC 3768 (Virtual Router Redundancy Protocol)
- RFC 3917 (IP Flow Information Export [IPFIX])
- RFC 3954 (Netflow Services Export v9)
- RFC 3993 (DHCP Subscriber-ID suboption)
- RFC 4250 (The Secure Shell [SSH] Protocol Assigned Numbers)

- RFC 4251 (The Secure Shell [SSH] Protocol Architecture)
- RFC 4252 (The Secure Shell [SSH] Authentication Protocol)
- RFC 4253 (The Secure Shell [SSH] Transport Layer Protocol) -
- RFC 4254 (The Secure Shell [SSH] Connection Protocol)
- RFC 4541 (Considerations for Internet Group Management Protocol [IGMP] and Multicast Listener Discovery [MLD] Snooping Switches)
- RFC 4604 (Using Internet Group Management Protocol Version 3 [IGMPv3])
- RFC 4673 (RADIUS Dynamic Authorization Server MIB)
- RFC 5905 (Network Time Protocol Version 4)

IPv6 specific RFCs

The following lists supported IPv6 specific RFCs:

- RFC 1886 DNS Extensions to support IPv6
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IPv6
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 3162 RADIUS and IPv6
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IPv6 Addressing Architecture

The following table lists partially supported IPv6 specific RFCs:

Table 9: Partially Supported IPv6 specific RFCs

Standard	Description	Compliance
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 2462	Auto-configuration of link local addresses	Supports creation of link-local addresses in section 5.3, and duplicate address detection in section 5.4.
RFC 4007	Scoped Address Architecture	Supports some behavior such as source address selection when transmitting packets to a specific

Table continues…

Standard	Description	Compliance
		scope, but there is not a zone concept in the code.
RFC 4022	Management Information Base for TCP	Mostly supported.
RFC 4113	Management Information Base for UDP	Mostly supported.
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack. No support for tunneling yet.
RFC 4291	IPv6 Addressing Architecture	Supports earlier version of RFC (3513).
RFC 4293	Management Information Base for IP	Mostly supported.
RFC 4443	Internet Control Message Protocol (ICMPv6)	Supports earlier version of RFC (2463).

Chapter 4: Resolved issues

Use the information in this section to learn more about issues that have been resolved in Release 5.7.3.

Reference number	Description
ERS454800–708 (wi01185798)	ERS 4800 v5.7.0: 5 out of 8 switches in a stack had rebooted due to Software Exception
ERS454800-807 (wi01219533)	ERS4500: v5.7.1 "NVR CFM: ERROR adding port filters" on non-SPB system
ERS454800-833 (wi01221188)	Two UBP filters applied to a port for the same PC blocking user traffic
ERS454800-868 (wi01224213)	100BASE-FX(LC) - AA1419074-E6 not working
ERS454800-904 (wi01226443)	High CPU after upgrading to 5.7/5.8 with the NAC server configuration
ERS454800-940 (wi01228738)	Switch sending an unexpected EAP Identity Request packet during EAP-TLS handshake causing authentication failure
ERS454800-1024	ERS 4500---Base unit is sending request for IP to DHCP using its own MAC instead of stack MAC
ERS454800-1175	DHCP Snooping - Binding Table not updated properly
ERS454800-1210 (wi01221845)	DHCP packets are copied to CPU due to dhcp-relay enabled globally and getting dropped
ERS454800-1233	High CPU during SNMPv3 polling
ERS454800-1234	Error generated from switch while exiting the SSH session
ERS454800-1235	Stack reboots with error ‘Task tMCMgr, Type Instr Access’ and ‘Task tMCMgr, Type Data Access’

Chapter 5: Known Issues and Limitations

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

Known issues and limitations for Release 5.7.3

The following table lists known issues and limitations for Avaya Ethernet Routing Switch 4000 Series Software Release 5.7.3.

For known issues prior to this release, see previous release notes available from the Avaya Support web site: www.avaya.com/support.

Reference number	Description
ERS454800-1046	EAP is configured with various settings for some stack ports when switching between 5.7.2.013 and 5.7.3.011. After upgrading to 5.7.3 from another 5.7.x image, some EAP settings may appear in running config in certain situations. This is due to version 5.7.3 modifying a structure that is also used by 5.7.x.
ERS454800-1057	LACP links on the base unit (BU) are disabled after the base unit is powered down and back up when the Fabric Attach Proxy is a three unit stack. When using Fabric Attach (FA), the uplink to the FA server is dynamically added to various VLANs. In a scenario where all LACP ports are aggregated by using the same VLAN membership, after rebooting the base unit, some ports from LACP are disabled. The dynamic VLAN membership for those ports are cleared once the unit is rebooted. WORKAROUND: Use MLT instead of LACP to avoid this situation.
ERS454800-1115	NEAP client continuously re-authenticated after `clear eapol non-eap` command. In an FA Proxy topology, if a binding for NEAP client is rejected by the FA server for any reason, the entry for the NEAP client will be deleted on the proxy device. If traffic from the client is seen on the proxy device, the re-authentication process starts over, leading into a continuous authentication process. In order to avoid a stress on the RADIUS server, Avaya recommends default `lldp tx-interval` settings.

Table continues…

Reference number	Description
	The reject reason which can trigger this continuous re-authentication under traffic can be legitimate, such as a wrong vid/isid pairing or a known issue on the server (VOSS FA server does not support I-SID zero binding requests when local VLAN exists, expecting to support this and allow C-VLAN join or C-VLAN to ELAN transition when zero I-SID:VLAN bindings are requested and local non-zero I-SID:VLAN already exists).

IPv6 limitations

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

Table 10: IPv6 limitations

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

Chapter 6: Booting with an ASCII configuration file from the local file system

This chapter provides conceptual and procedural information to help you use this feature on ERS 4000 Series switches introduced in Release 5.7.3.

Booting with an ASCII configuration file from the local system

This feature allows you to download an ASCII configuration file from a TFTP server or USB to the local file system and boot the system with the local ASCII configuration file. Two ASCII configuration files are supported, one in each block. When you download and save an ASCII configuration file to the local file system, the system deletes the old file in that block.

For ERS 4500, the maximum size of an ASCII configuration file is limited to 150 kilobytes.

Once the system boots successfully with an ASCII configuration file, the system configuration is saved to the binary configuration. If the boot fails, the system resets and boots with the current binary configuration.

Note:

Downgrading software from one major release to another (e.g. Release 5.7 to 5.6) deletes all the ASCII files from the local ASCII file system, whereas downgrading from a minor release to another minor release (e.g. 5.7.4 to 5.7.3) does not delete the ASCII files.

Additionally, using the **boot default** command does not delete the ASCII files from the ASCII file system.

Displaying the ASCII configuration file status

About this task

Use this procedure to view the status of the ASCII configuration file.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show script block
   ```

3. Press Enter.

Example

```
Switch(config)#show script block

-------------------------------------------------------
Block  Name               Last Used   Last Status
-------------------------------------------------------
1      script_block_1     YES         Pass
2      script_block_2     NO          Fail
```

Variable definitions

The following table describes the fields in the `show script block` command.

Variables	Description
Block	Specifies the block assigned to the ASCII configuration file when downloaded.
Name	Specifies the name for the local ASCII configuration file. If no ASCII configuration files have been downloaded, this field remains blank.
Last Used	Indicates whether an ASCII configuration file was used the last time the system was booted.
Last Status	Indicates the status of the last execution, either Pass or Fail. If an ASCII configuration file was not used, this field displays Fail.

Downloading an ASCII configuration file from a TFTP server or USB device

About this task

Use this procedure to download an ASCII configuration file from a TFTP server or USB device to the local ASCII file system. You can then boot the system from the local file system. In a stack, the downloaded ASCII configuration file will be saved in all units.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To download from a TFTP server, enter the following command at the command prompt:

   ```
   copy tftp script address <address> filename <filename> block <1-2>
   [name <name>]
   ```

3. To download from a USB device, enter the following command at the command prompt:

   ```
   copy usb script filename <filename> block <1-2> [name <name>]
   ```

Next steps

Proceed with the `boot script` command to boot the system with the local ASCII configuration file.

Once the system boots successfully with an ASCII configuration file, the system configuration is saved to the binary configuration. If the system boot fails, the system resets and boots with the current binary configuration.

For the boot command, see Setting boot parameters on page 49.

Variable definitions

Variable	Description
address *<A.B.C.D>* | *<WORD>*	Specifies the address of the TFTP server to load the script. • A.B.C.D - specifies the IPv4 address • WORD - specifies the IPv6 address
filename *<WORD>*	Specifies the name of the file to be retrieved.
block *<1–2> [name <WORD>]*	Specifies the block from which the ASCII configuration file is to be downloaded. If you do not specify a name for the block name, the default is the name of the file retrieved.

Setting boot parameters

About this task

Use this procedure to boot the switch or stack and to set boot parameters. This command is used to perform a soft-boot of the switch or stack.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   boot [default [unit <1-8> ] | nvram block <1-2> | partial-default |
   script block <1-2> | unit <1-8>]
   ```

3. Press Enter.

   Important:

   When you reset the switch or stack to factory default, the switch or stack retains the stack operational mode, the last reset count, and the reason for the last reset; these three parameters are not reset to factory defaults.

   Important:

   When you reset the switch or stack to factory partial-default, the switch or stack retains the following settings from the previous configuration:

   - IP information
     - IP address
     - subnet mask
     - default gateway
     - bootp mode
     - last bootp IP address
     - last bootp subnet mask
     - last bootp gateway
     - IPV6 management interface address
     - IPV6 default gateway
   - software license files
   - passwords for console and Telnet/WEB

   RADIUS and TACACS authentication settings are not retained. If the console password type is set to local, RADIUS, or TACACS+, after reset, the console password type is set to local.

Variable definitions

The following table describes the variables for the `boot` command.

Variables	Description
default	Restores switch or stack to factory-default settings after rebooting.
nvram block <1–2>	Reboots with the binary configuration data in NVRAM using the block specified.
partial-default	Reboots the stack or switch and use factory partial-default configurations. **Note:** You can use the boot partial-default command on a standalone switch or on an entire stack. You cannot reset individual units in a stack to partial-default.
script block <1–2>	Reboots with the ASCII configuration file using the binary configuration block specified.
unit <unit no>	Specifies which unit of the stack is rebooted. This command is available only in stack mode. Enter the unit number of the switch you want to reboot.