Release Notes for Avaya Ethernet Routing Switch 5000 Series

Release 6.6.3
NN47200-400
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/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

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

License types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at 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 for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: 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

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) and a list of resolved issues. This document also describes known limitations and expected behaviors that may first appear to be issues.

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for the Avaya Ethernet Routing Switch 5000 Series, Release 6.6 and higher.

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

See the *Documentation Reference for Avaya Ethernet Routing Switch 5000 Series*, NN47200–103 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

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 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

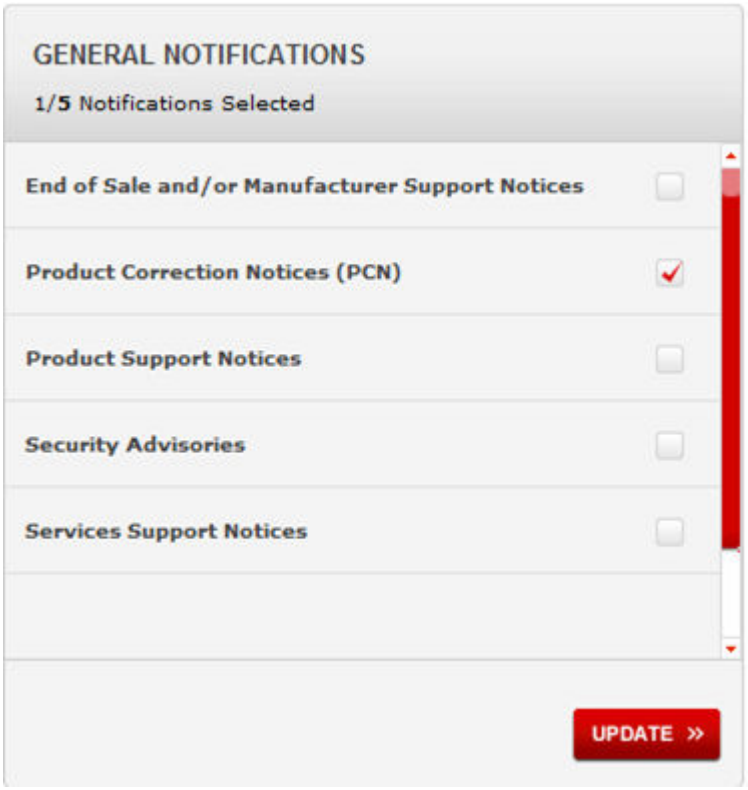
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

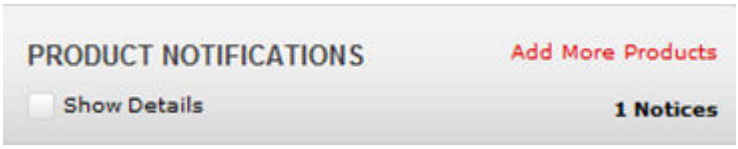
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services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

Procedure

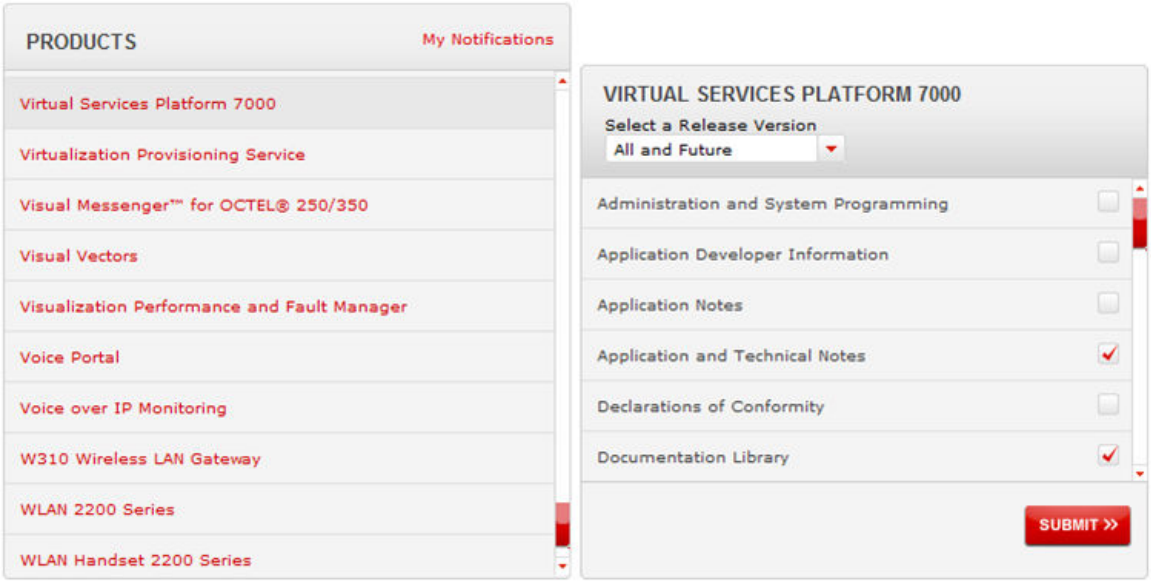
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click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

Supported Switch Models

The Avaya Ethernet Routing Switch 5600 Series, supported by software release 6.6, includes the following switch models:

- Avaya Ethernet Routing Switch 5698TFD
- Avaya Ethernet Routing Switch 5698TFD-PWR
- Avaya Ethernet Routing Switch 5650TD
- Avaya Ethernet Routing Switch 5650TD-PWR
- Avaya Ethernet Routing Switch 5632FD

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, with the restriction that the maximum number of ports supported in a stack is 400 ports. One of the benefits of operating Avaya Ethernet Routing Switch

5600 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.

Note:

Release 6.6 supports pure stacks of 56xx switches only. Hybrid or mixed stacking of 55xx with 56xx switches and pure stacks of 55xx switches are not supported.

Chapter 2: New in this release

The following sections detail what's new in *Avaya Ethernet Routing Switch 5000 Series Release Notes* — Software Release 6.6.3.

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 5000 Series*, NN47200–513.

Chapter 3: Important notices and new features

This section describes important software and hardware related notices in the Avaya Ethernet Routing Switch 5000 Series for this release.

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
QoS Traffic Profiling Support	*Configuring Quality of Service on Avaya Ethernet Routing Switch 5000 Series*, NN47200-504
SMLT configuration	*Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 5000 Series*, NN47200–502

Release file names

The following table describes the Avaya Ethernet Routing Switch 5000 Series software components for this release.

Table 2: Release 6.6.3 software components

File Type	Description	File Name	File Size (bytes)
Standard runtime image software version 6.6.3	Standard non SSH image for the Ethernet Routing Switches 5000 Series	5xxx_663014.img	10,847,396

Table continues…

File Type	Description	File Name	File Size (bytes)
Secure runtime image software version 6.6.3	Standard SSH image for the Ethernet Routing Switches 5000 Series	5xxx_663015s.img	11,114,404
Diagnostic software version 6.0.0.18	ERS5600 diagnostic software	5xxx_60021_diags.bin	2,472,272
Enterprise Device Manager Help Files	EDM Help files zip	ers5000v663_HELP_EDM.zip	2,081,001
MIB Definition File	MIB Definition File	Ethernet_Routing_Switch_5xxx_MIBs_6.6.3.zip	1,660,270
COM Plug in	ERS5600 plugin for COM	ers5000v6.6.3.0.zip	3,494,461

Software upgrade

The procedures in this section are used to upgrade the diagnostic and agent software. Use these procedures to upgrade to Software Release 6.6 and higher.

Important:

There is no upgrade path from any agent software release earlier than 6.3 to Software Release 6.6. Devices running older agent software must first be upgraded to a version of Software Release 6.3 before upgrading to Software Release 6.6. Note that the diagnostic software running on the device should not be earlier than 6.0.0.16.

Important:

If upgrading from a 5.x diagnostic image to a 6.x diagnostic, you should not use the no-reset option. You must execute the 6.x diagnostic prior to loading any 6.x agent images.

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.

Table continues…

Parameter	Description
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. • To load the agent image if it is a PoE module image, use the poe_module_image option.

Table continues…

Parameter	Description
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.

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

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

Upgrade strategy	Upgrade all switches in your network if the switches are running software versions prior to the versions mentioned in the following: • ERS 25xx: 4.4.3. **Note:** Note: ERS 25xx is in End of Sales and currently there is no schedule planned for 4.4.3 software version. • ERS 35xx: 5.1.2, 5.2.x • ERS 4xxx: 5.6.4, 5.7.1, 5.8.x • ERS 5xxx: 6.2.8, 6.3.3, 6.6.x • VSP 7xxx: 10.3.2, 10.4.x **Note:** Upgrade the affected ERS switches closest to the client devices first and then progress towards the core.
Issue	In some previous software releases of the Stackable ERS platforms (ERS 2500, 3500, 4000 and 5000 Series) as well as the VSP 7000, a software issue

Table continues…

	was found to cause malformed DHCP packets as they were forwarded out of the switch. In the software releases listed in the preceding row, a code change has been made to stop the malformed packets from being generated and also to discard these malformed packets if the switch is receiving them. Due to the nature of the code change, there are potential interaction scenarios between ERS switches running different code versions which will need to be managed within the context of a network upgrade to releases containing the code changes.
Implications if this upgrade strategy is not followed	DHCP packets which previously transitioned the network without issue may now be lost if using ERS switches which utilize mixed agent versions with and without this fix.
Workaround if this upgrade strategy is not followed	• Disable the DHCP features (DHCP snooping, DHCP relay or DHCP signature authentication) on switches running the older software versions so that the malformed DHCP packets are not generated. Implementation of this option is dependent on the network topology that still allows DHCP packets to reach the DHCP server and may require additional configuration changes. • Disabling DHCP snooping or DHCP relay on switches running the software with the fix will prevent malformed DHCP packets from being dropped if they are received from other switches that are not upgraded. Implementation of this option may also require additional configuration changes to ensure that the DHCP requests reach the DHCP server.

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

How to get EDM online help files for embedded EDM

Because 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. Once 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 files 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 *Fundamentals of Avaya Ethernet Routing Switch 5000 Series*, NN47202-104.

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 ERS5000_66_Help tftp address 100.100.100.15
```

In the preceding example ERS5000_66_Help is a folder that contains help files and 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 5000 Series, Release 6.6 and higher, and Enterprise Device Manager.

Table 3: Supported software and hardware capabilities

Feature	Maximum number supported
VLANs	1024 (1k)
Protocol-based VLANs	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 5000 Series*, NN47200–502 for more information.
IGMP maximum number of unique groups	Layer 2 and Layer 3 992
EAPoL 802.1x supplicants	32 per port 768 per stack
Maximum number of routes (dynamic, static and local)	4000 routes for ERS 5600 units and stacks
ARP records	4096
Static ARP	256
IP interfaces	256
Static routes	512
Spanning Tree Groups	8
IPv6 DHCP relay forward paths	256
IPv6 static routes	512
IPv6 interfaces	256
IPv6 tunnels	4
Aggregation groups (link aggregation)	32
Ports per aggregation group	8
MAC addresses in fdb	16 K
OSPF areas	4 (3 areas plus area 0)
OSPF adjacencies	64
VRRP interfaces	64
ECMP	4 paths
DHCP Snooping Binding table entries	1024 per switch
DHCP relay forward paths	512
IP Management routes	4
PIM-SM multicast entries	Up to 992 for ERS 56xx series The ERS 56xx platforms support a maximum of 992 IPMC forwarding entries.

Table continues…

Feature	Maximum number supported
	These limitations are imposed on standalone ERS 56xx devices and stacks. Note: These limits do not indicate that 992 entries will actually be available since the installation of IPMC entries in hardware is also determined by free entries being available.
Allow-flood IGMP multicast addresses	The maximum number of allow-flood multicast entries is determined by the number of VLANs on the device. Each entry in the allow-flood table applies to each current VLAN; for example, if 1 entry exists in the allow-flood table and 5 VLANs are configured, then there are 5 entries programmed in hardware. Currently, the hardware limit is 4096. Note: You should not exceed this limit. The limit for the maximum number of allow-flood addresses is 128 (1 VLAN).
Link State Tracking: Instances	2
Port Mirroring: Instances	4
Port Mirroring: RSPAN VLANs	4
Port Mirroring: RSPAN destinations	4 per switch or stack
VRF: Instances	4
Neap supplicants	32 per port 768 per stack

Additional information for the software feature license file

When you create a license file to enable licensed features on an Avaya Ethernet Routing Switch 5000 Series switch with the Avaya Electronic Licensing Portal, you must specify a file name. Follow the instructions on the License Certificate within the License Kit, or for more information, see *Fundamentals of Avaya Ethernet Routing Switch 5000 Series*, NN47202-104.

You must use the following rules when you generate and name the file:

- A maximum of 63 alphanumeric characters
- Lower case only
- No spaces or special characters allowed
- Underscore (_) is allowed
- The dot (.) and three-character file extension are required

File name example, abcdefghijk_1234567890.lic.

The format of the file that you upload to the license generation tool, and that contains the list of MAC addresses, must be as follows:

- ASCII file format
- One MAC address per line
- No other characters, spaces, or special characters allowed
- MAC must be in hexadecimal, capitalized format, with each pair of characters separated by colon; for example, XX:XX:XX:XX:XX:XX
- The file must contain the correct MAC addresses. Any incorrect MAC addresses will result in the licensed features not working on designated units.
- The number of MAC addresses must not exceed the number of MAC addresses allowed for the License Authorization Code entered for a particular file. For example:
  - AL1016001 = 2 MAC addresses (1 stack/standalone unit)
  - AL1016002 = 20 MAC addresses (10 stacks/standalone units)
  - AL1016003 = 100 MAC addresses (50 stacks/standalone units)
  - AL1016004 = 200 MAC addresses (100 stacks/standalone units)

Supported standards, MIBs, and RFCs

This section lists the standards, MIBs, and RFCs supported by the Avaya Ethernet Routing Switch 5000 Series.

Standards

The following IEEE Standards contain information that applies to the Avaya Ethernet Routing Switch 5000 Series:

- 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)
- RFC 1271 (RMON)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 1757 (RMON)
- RFC 1945 (HTTP v1.0)
- RFC 2131 (DHCP)
- RFC 2236 (IGMPv2)
- RFC 2362 (PIM-SM)
- RFC 2474 (QoS)
- RFC 2597 (QoS)
- RFC 2598 (QoS)
- RFC 2665 (Ethernet MIB)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2865 (RADIUS)

- RFC 3140 (QoS)
- RFC 3246 (QoS)
- RFC 3376 (IGMPv3)
- 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 3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service)

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
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

Table continues…

Standard	Description	Compliance
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.

Change Request Number	Description
Resolved issues in Release 6.6.3	
ERS555600-1062 (wi01213024)	ERS5698TFD-PWR 2 unit stack under high CPU on upgrading from v6.2.0 to v6.6.1
ERS555600-1139	ERS 5650 - IST didn't come up after migration from 6.3.5 to 6.6.1 software
ERS555600-1137	TCP FYN not generated from switch while exiting the SSH session.

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

See the following table for a list of known issues for the Avaya Ethernet Routing Switch 5000 Series.

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

Table 4: Known issues

Reference number	Description
Known issues from Release 6.6.3	
ERS555600-1149	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.
ERS555600-1223	EAP is configured with various settings for some stack ports when switching between 6.6.2.013 and 6.6.3.009.. After upgrading to 6.6.3 from another 6.6.x image, some EAP settings may appear in running config in certain situations. This is due to version 6.6.3 modifying a structure that is also used by 6.6.x.
ERS555600-1224	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

Table continues…

Reference number	Description
Known issues from Release 6.6.3	
	stress on the RADIUS server, Avaya recommends default `lldp tx-interval` settings. 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).

Trap restoration and reconfiguration after upgrade to Release 6.3

Use the procedures in this section to restore and reconfigure trap functionality after you upgrade to Release 6.3 software. You can reconfigure trap notification, using either EDM or ACLI.

Restoring trap notification functionality using ACLI

About this task

Use the following procedure to restore trap notification functionality using ACLI:

Procedure

Use the following ACLI command to remove traps created using R6.1 and before: **`no snmp-server host X.Y.Z.T 'community name'`**

Reconfiguring traps using EDM

About this task

Use the following procedure to reconfigure traps using 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.

Reconfiguring traps using ACLI with v1 host example, password security enabled

About this task

Use the following procedure to reconfigure traps using ACLI - v1 host example with password security enabled:

Procedure

1. To create a community, from the Global Configuration prompt, enter the following command:

   ```
   snmp-server community notify-view nncli
   ```

   Enter community string: CommunityName

   Enter community string: CommunityName

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`.

Reconfiguring traps using ACLI with v1 host example, password security disabled

About this task

Use the following procedure to reconfigure traps using ACLI - v1 host example with password security disabled:

Procedure

1. To create an SNMP community, from the Global Configuration prompt, enter the following command: `snmp-server community CommunityName notify-view nncli`.
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`.

Setting the Notification Type per receiver using ACLI

About this task

Use the following procedure to set the Notification Type per receiver using 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`.

Displaying Notification Types associated with the notify filter using ACLI

About this task

Use the following procedure to display the Notification Types associated with the notify filter using ACLI.

Procedure

From the Global Configuration prompt, enter the following command: `show snmp-server notification notify filter`

Enabling or disabling the Notification Type per device using ACLI

About this task

Use the following procedure to enable or disable the Notification Type per device using 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`.

Preventing a loop during upgrade of a large network

About this task

Use the following procedure to prevent a temporary loop during upgrade of a large network.

Procedure

1. Shut down LAC/SMLT ports on system A.
2. Download the new software image to system A.
3. Enable LAC/SMLT ports on system A.
4. Shut down LAC/SMLT ports on system B.
5. Download the new software image to system B.
6. Enable LAC/SMLT ports on system B.

Ethernet Routing Switch 5000 Series limitations and considerations

The following table lists known Ethernet Routing Switch 5000 Series limitations and considerations:

Table 5: Ethernet Routing Switch 5000 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	Avaya recommends that you 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 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.
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."

Table continues…

Item	Description
	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	Release 5.1 introduced a Demo License to enable OSPF, ECMP, VRRP, SMLT, and IPFIX for a period of 30 days. The trial license expires at the end of the 30-day period and the features, except SMLT, are disabled. The system sends traps advising of license expiration but SMLT remains enabled until the stack or unit is reset. Avaya recommends that, when you receive the first trap, the administrator begins to manually disable SMLT and ensure removal of any cabling loop. Because Spanning Tree Protocol needs to be disabled and, because SMLT is implemented through cabling, SMLT is not disabled with the other features because a network loop would form. After demo license expiry, when the stack or unit is reset, SMLT is disabled and a loop will form if there has been no intervention to remove or disable the ports participating in the IST. 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	Avaya recommends that you do not enable IP Source Guard on trunk ports.
10	Avaya recommends that you do not enable Critical-IP functionality with VRRP in an SMLT environment.
11	Lossless Mode: Lossless activates in oversubscription scenarios even if rate-limiting is applied to certain ingress streams and slowing them is not necessary. Lossless gives fair access to bandwidth, meaning that if you have 3 ingress streams of 100% line rate competing on 1 egress port, lossless will slow down the sender transmit rates to a 33-33-33 percentage, and it does this by sending pause frames. If you have 2 streams coming in at 100% and a third at 20%, lossless will not interfere with this stream, the egress percentages will be 40-40-20. If the third stream transmit rate exceeds 33%, lossless will begin to apply to it as well. In this situation, if applying a meter to this stream, limiting it at under 33%, lossless doesn't activate and doesn't interfere. However, if the third stream is either broadcast or multicast traffic and a rate-limiting setting is applied instead of a meter, lossless will activate - it will send pause frames to the sender. The egress rate of the stream is not affected, it will be the one imposed by the rate-limiting setting, but the transmit rate will vary because of the pause frames.
12	Lossless Mode: In Lossless buffering mode, if you use ingress traffic with queue 1 + ingress traffic with queue 2, and the egress port is on a different asic from ingress ports, QoS queue shaper may limit the bandwidth for queue 1 under the min-rate and egress traffic may be under the expected rates.
13	ARP Table Size for ERS 5600: The maximum number of entries in the ARP table is 4096.
14	MAC Filtering List: Release 6.3 of ERS 5000 increases the maximum number of entries in the MAC Filtering List to 128. More upper limit testing is required.

Table continues…

Item	Description
15	Inexistent VLAN Mapping for MSTI: EDM/SNMP support for VLAN Mapping for MSTI is not available in Release 6.3.
16	In Release 6.3, the LLDP default settings for lldp tx-tlv and lldp tx-tlv med have been changed to enabled. In prior releases, the default setting for LLDP was disabled. These settings only apply when the switch is defaulted or the default LLDP setting is applied. When upgrading from a previous version, the configured LLDP settings will be retained.

17	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.`

18	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
19	In a stack configuration, SSHC configuration options are only available from the base unit

20	When you manually create an LLPD 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`

VLACP issue

In some situations, when you use VLACP the ERS 5000 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 5600 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 ERS 5600 switches

maintain a rolling history of the last 3 received VLACP PDUs (by default) and calculate the time variance across and between these VLACP messages.

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

Filter resource consumption

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

A filter specifies the bit pattern to match.

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

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

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

Table 6: Application mask and filter resource requirements

Application	Category	Masks required	Filters required
Ethernet Routing Switch 5600 Series			
Broadcast ARP and ARP Inspection	Non QoS	1	1
DHCP Relay or DHCP Snooping	Non QoS	1	2
QoS (default untrusted policy)	QoS	2	2
QoS (DAPP with status tracking)	QoS	1	1
QoS (Auto QoS)	QoS	1	4
Port Mirroring (MAC-based)	Non QoS	1	2
EAP Authetication (EAPoL packet filter)	Non QoS	1	2
IPFIX	Non QoS	1	1
ADAC	Non QoS	1	1
RIP	Non QoS	1	1
UDP Broadcast	Non QoS	1	1
BGP (ERS 5600 only)	Non QoS	1	2
VRRP	Non QoS	1	2

Table continues…

Application	Category	Masks required	Filters required
OSPF	Non QoS	1	2
Content Based Forwarding (ERS 5600 only)	Non QoS	1	1
IP Source Guard	Non QoS	1	11
PIM	Non QoS	1	1

On the ERS 5600 Series switches the resources are shared across groups of ports. For each group of ports there 16 masks and 256 filers available for each mask. By default, the system consumes 2 masks and 2 filters for ARP filtering and DHCP relay on all ports, leaving 14 masks available for each group and 254 filters available for each mask and group 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 ERS 5000 Series 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 ERS 5600 Series switches, 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 5600 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 5600 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 5600 Series switch port

On ERS 5600 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 / autonegotiation advertisement). When upgrading from an older software version (that had symmetic as default), the symmetric/pause-frame settings are changed to asymmetric/asymm-pause-frame.

Example

Disabling flow control when autonegotiation is enabled:

```
ERS>enable
ERS#configure terminal
ERS(config)#interface ethernet 7-8
ERS(config-if)#auto-negotiation-advertisements port 7 1000-full
ERS(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
---- ---------------------------------------------------------------
7                                  1000Full
8    10Full 10Half 100Full 100Half 1000Full              AsymmPause
ERS(config-if)#show interfaces 7-8
               Status          Auto                          Flow
Port Trunk Admin  Oper  Link Negotiation  Speed  Duplex Control
---- ----- ------ ----  ---- -----------  -----  ------ -------
7          Enable Up    Up   Custom       1000Mbps Full Disable
8          Enable Up    Up   Enabled      1000Mbps Full Disable
```

Enabling asymmetric flow control when autonegotiation is enabled:

```
ERS>enable
ERS#configure terminal
ERS(config)#interface ethernet 7-8
ERS(config-if)#auto-negotiation-advertisements port 7 1000-full asymm-pause-frame
ERS(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
---- ---------------------------------------------------------------
7                                  1000Full              AsymmPause
8    10Full 10Half 100Full 100Half 1000Full              AsymmPause
ERS(config-if)#show interfaces 7-8
               Status          Auto                          Flow
Port Trunk Admin  Oper  Link Negotiation  Speed  Duplex Control
---- ----- ------ ----  ---- -----------  -----  ------ -------
7          Enable Up    Up   Custom       1000Mbps Full Asymm
8          Enable Up    Up   Enabled      1000Mbps Full Asymm
```

Disabling flow control when autonegotiation is disabled:

```
ERS>enable
ERS#configure terminal
ERS(config)#interface ethernet 7-8
ERS(config-if)#duplex port 7-8 full
ERS(config-if)#flowcontrol port 7-8 disable
ERS(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 autonegotiation is disabled:

```
ERS>enable
ERS#configure terminal
ERS(config)#interface ethernet 7-8
ERS(config-if)#flowcontrol port 7-8 asymmetric
ERS(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
```