Release Notes for Avaya Ethernet Routing Switch 3500 Series

Release 5.2
NN47203-400
Issue 04.02
March 2014

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. “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.

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.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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.

Contents

Chapter 1: Introduction

Purpose

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for Avaya Ethernet Routing Switch 3500 Series, Software Release 5.2.

Related Resources

Documentation

For a list of the documentation for this product, see *Avaya Ethernet Routing Switch 3500 Documentation Road Map* (NN47203–101).

Support

Visit 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.

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.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://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 site.

Note:

Videos are not available for all products.

Training

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

Chapter 2: New in this release

New in this release

The following sections detail what is new in Avaya Ethernet Routing Switch 3500 Series for Release 5.2.

These Release Notes are a supplement to the technical documentation and, in some cases, may supersede information contained in them.

Hardware

The following table lists and describes the hardware that is new for the Avaya Ethernet Routing Switch 3500 Series Release 5.2:

Table 1: Switch models

Model	Description
Avaya Ethernet Routing Switch 3549GTS	48 10/100/1000 non-PoE and 2 shared SFP, plus 1 1/10 Gigabit SFP+ port, plus 2 rear dual mode/stacking ports.
Avaya Ethernet Routing Switch 3549GTS-PWR+	48 10/100/1000 802.3at PoE+ and 2 shared SFP, plus 1 1/10 Gigabit SFP+ port, plus 2 rear dual mode/stacking ports.

Table 2: Avaya 10 GB SFP+ devices

Model	Description
AA1403011-E6	10GBT-LR SFP+ (LC) SINGLE MODE 10 km
AA1403013-E6	10GB-ER SFP+ (LC) SINGLE MODE 40 km
AA1403015-E6	10GB-SR 850 nm
AA1403016-E6	10GBase-ZR/ZW 70 km
AA1403017-E6	10GB-LRM SFP+ (LC) MULTI-MODE, 220 m
AA1403018-E6	SFP+ direct attach cable, 10 m
AA1403019-E6	SFP+ direct attach cable, 3 m

Model	Description
AA1403020-E6	SFP+ direct attach cable, 5 m
AA1403153-E6	CWDM SFP+ LC - 1470 nm Wavelength, 40 km
AA1403154-E6	CWDM SFP+ LC - 1490 nm Wavelength, 40 km
AA1403155-E6	CWDM SFP+ LC - 1510 nm Wavelength, 40 km
AA1403156-E6	CWDM SFP+ LC - 1530 nm Wavelength, 40 km
AA1403157-E6	CWDM SFP+ LC - 1550 nm Wavelength, 40 km
AA1403158-E6	CWDM SFP+ LC - 1570 nm Wavelength, 40 km
AA1403159-E6	CWDM SFP+ LC - 1590 nm Wavelength, 40 km
AA1403160-E6	CWDM SFP+ LC - 1610 nm Wavelength, 40 km
AA1403161-E6	CWDM SFP+ LC - 1470 nm Wavelength, 70 km
AA1403162-E6	CWDM SFP+ LC - 1490 nm Wavelength, 70 km
AA1403163-E6	CWDM SFP+ LC - 1510 nm Wavelength, 70 km
AA1403164-E6	CWDM SFP+ LC - 1530 nm Wavelength, 70 km
AA1403165-E6	CWDM SFP+ LC - 1550 nm Wavelength, 70 km
AA1403166-E6	CWDM SFP+ LC - 1570 nm Wavelength, 70 km
AA1403167-E6	CWDM SFP+ LC - 1590 nm Wavelength, 70 km
AA1403168-E6	CWDM SFP+ LC - 1610 nm Wavelength, 70 km

Avaya recommends that you use Avaya SFP and SFP+ devices to provide maximum compatibility and support for the ERS 3500 Series. The following third-party SFP+ devices are validated by Avaya to function only with the 3549GTS/GTS-PWR+ SFP+ port.

Table 3: Third-party 10 GB SFP+ devices

Vendor	Model	Description
Cisco	450–16141	SFP+ direct attach cable, 5 m
Cisco	450–16140	SFP+ direct attach cable, 3 m
Cisco	450–16142	SFP+ direct attach cable, 1 m
Hewlett-Packard	J9281B	SFP+ direct attach cable, 1 m
Hewlett-Packard	J9283B	SFP+ direct attach cable, 3 m
Hewlett-Packard	J9285B	SFP+ direct attach cable, 7 m

Features in Release 5.2

See the following sections for information about feature changes in release 5.2.

Avaya Energy Saver

Avaya Energy Saver (AES) can reduce network infrastructure power consumption without impact to network connectivity. AES reduces direct power consumption by up to 40% because it uses intelligent switching capacity reduction in off-peak mode. AES can also use Power over Ethernet (PoE) port power priority levels to shut down PoE ports and provide more power savings.

You can configure AES using ACLI or EDM. For more information, see *Getting Started with Avaya Ethernet Routing Switch 3500 Series*, NN47203-301.

Secure SLA Monitor agent-server communication

The Avaya ERS 3500 supports the Service Level Agreement (SLA) Monitor agent as part of the Avaya SLAMon solution. SLAMon uses a server and agent relationship to perform end-to-end network Quality of Service (QoS) validation, and acts as a distributed monitoring device. You can use the test results to target under-performing areas of the network for deeper analysis.

The secure SLA Monitor agent-server communication feature supports certificate-based authentication and encrypted agent-server communication. The communication mode is based on the ERS image.

Release 5.1 supports non-secure communication with the Avaya Diagnostic server, while Release 5.1.1 supports secure communication with the server. Secure images (Release 5.1.1 and later) use authentication/encryption and non-secure images (prior to Release 5.1.1) use clear text communication.

During registration, an X.509 certificate is retrieved from the server and then validated against the stored Avaya CA certificate. If the received certificate is trusted, a secure channel is established. A symmetric encryption key is exchanged and used for all subsequent agent-server communications.

Note:

The certificate-based authentication and encrypted agent-server communications are automatically enabled on secure ERS images. This is not a user configuration feature.

In Release 5.2, in addition to certificate-based authentication and encrypted communication, you can perform New Trace Route (NTR) and Real-Time Protocol (RTP) tests on the local agent using CLI.

For more information, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 3500 Series*, NN47203-501.

SLPP Guard

You can use Avaya's Split Multi-Link Trunking (SMLT) in combination with Simple Loop Prevention Protocol (SLPP) Guard to provide additional loop protection to protect wiring closets from erroneous connections. SMLT implementations provide an SLPP packet which helps prevent loops from occurring when switch clustering is implemented.

When you enable SLPP Guard, this loop prevention mechanism is extended into and across multiple wiring closets. If the edge switch configured for SLPP Guard receives an SLPP packet on a port, the feature can immediately disable the port administratively, and generate the appropriate log messages and SNMP traps.

Note:

SLPP packets are generated only on switches that are configured with SLPP. For example, ERS 5000 Series or ERS 8300 switches. The ERS 3500 switches do not support SLPP. When you enable SLPP Guard on an ERS 3500, the switch must be connected to another Avaya switch that supports SLPP and SLPP must be enabled on that switch.

For more information, see *Configuring Layer 2 on Avaya Ethernet Routing Switch 3500 Series*, NN47203-500.

Static LACP key to trunk ID binding

Static LACP key to trunk ID binding provides you with more control over the association between LACP ports and trunk groups than dynamic binding. For backwards compatibility, both static LACP key to trunk ID binding and dynamic binding are available. However, when the static method is set, it overrides the dynamic method.

With Static LACP Key to Trunk ID binding, you associate a specific group of link-aggregated ports with a specific MLT trunk group. The static binding ensures that the switch maintains the LACP Key - MLT ID association until you delete the binding.

Note:

Avaya recommends you to use the Static LACP key to trunk ID binding because it can prevent undesired configurations. For example, if you configure two LACP trunks, the MLT IDs are assigned to each trunk in the order of their creation. If the device is rebooted, the LACP and VLACP fundamentals order that each LAG receives a trunk might invert and the LACP aggregator might receive a different trunk than what was intended. The Static LACP key to trunk ID binding feature association between LAGs and MLT IDs can prevent this problem.

Static LACP key to trunk ID binding is enabled by default. When configured, the Static LACP key - MLT ID binding overrides the dynamic association. If no binding settings are configured, the dynamic association applies.

Important:

With Static LACP key to trunk ID binding, you must keep track of the used trunk IDs. Binding multiple keys to different trunks may easily lead to the use of all available MLT IDs. If all MLT IDs are used, you cannot configure a new LACP trunk, even if all the other required conditions for trunk formation are accomplished.

Show Flash History

The FLASH history provides the current status of the FLASH device. Use the **`show flash history`** command to view the FLASH writes and erase history on a standalone unit or stack. The FLASH history does not record programming done from the diagnostics or bootloader. FLASH history is stored in system FLASH. The data does not get corrupted during an upgrade or downgrade. FLASH History is automatically enabled and does not require any configuration.

Unified Authentication

With the introduction of 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. When in stacked mode, the authentication method, username, and local passwords are applied universally across all switches in a stack.

If you use the `cli passwords` and `username` ACLI commands, the unified and previously used standalone authentication method, the username, and local passwords are updated on all switches in the stack.

The switch updates the obsolete standalone authentication method, username, and local passwords to ensure maximum compatibility, should it become necessary for you to downgrade the switch to a previous software release.

Other changes

See the following sections for information about changes that are not feature-related.

Power over Ethernet (PoE) support

The Avaya Ethernet Routing Switch 3500 Series 3526T-PWR+ (PoE switch) provides IEEE 802.3az-compliant power or PoE on all 10/100 RJ-45 ports.

The Avaya Ethernet Routing Switch 3500 Series 3510GT-PWR+, 3524GT-PWR+, and 3549GT-PWR+ (PoE switches) provide IEEE 802.3az-compliant power or PoE on all 10/100/1000 RJ-45 ports.

PoE support on Avaya Ethernet Routing Switch 3500 Series switches is backwards-compatible with IEEE 802.3af PoE and IEEE 802.3at PoE+.

Document title change

In Release 5.2, the title of this document changed from *Avaya Ethernet Routing Switch 3500 Series Release Notes*, NN47203-400 to *Release Notes for Avaya Ethernet Routing Switch 3500 Series*, NN47203-400.

Chapter 3: Important notices

Important notices

This section provides important software and hardware related notices.

File names for release 5.2

The following table describes the Avaya Ethernet Routing Switch 3500 Series, Software Release 5.2, software files. File sizes are approximate.

Module or file type	Description	File name	File size (bytes)
Standard (non-SSH) runtime image software version 5.2.0.4	Standard software image for the Avaya Ethernet Routing Switch 3500 Series	ERS3500_520004.img	8524580
Secure (SSH) runtime image software version 5.2.0.5	Standard software image for the Avaya Ethernet Routing Switch 3500 Series	ERS3500_520005s.img	8764932
Bootloader software version 1.0.0.4	Bootloader software for the Avaya Ethernet Routing Switch 3500 Series	ERS3500_b1_0_0_4.bin	225756
Diagnostic software version 1.0.0.12	Diagnostic software for the Avaya Ethernet Routing Switch 3500 Series	3500_10012_diag.bin	2095545
Software Release 5.2 MIB definition files	Management Information Base (MIB) definition files	Ethernet_Routing_Switch_35xx_MIBs_5.2.0.zip	1558432
EDM Help file zip	A downloadable zip file containing Help information for	ers3500v520_HELP_EDM.zip	3610038

Module or file type	Description	File name	File size (bytes)
	Enterprise Device Manager (EDM)		
COM Plug in file zip	COM Plug in for Enterprise Device Manager (EDM)	ers3500v5.2.0.0.zip	4399024

Upgrading the Diag image using ACLI

Perform the following procedure to upgrade the Diag image using ACLI.

Procedure

1. Connect a default switch to a TFTP server.
2. Set a valid IP address and subnet mask.
3. Configure the TFTP server address using the following command from Privileged EXEC mode:

   ```
   tftp-server <A.B.C.D>
   ```
4. Verify the connection to the TFTP Server.
5. At the command prompt, enter the **download** command with the following parameters.

   ```
   download diag <WORD>
   ```

   The Diag image is downloaded and then the switch is rebooted. To avoid rebooting the switch after the download, add the option *<no-reset>* to the **download** command.

Variable definitions

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

Variable	Value
<A.B.C.D>	Enter the IP address of the TFTP server in the format XXX.XXX.XXX.XXX
<WORD>	The filename of the diagnostic image

Updating the Diag image from the Boot menu

Use this procedure to update the Diagnostics image from the Boot menu.

Procedure

1. Connect a default switch to a TFTP server.
2. Reboot the switch (either a soft or hard reset).
3. During the boot process, press `CTRL+C` until the following menu is displayed:
   a. Press `'a'` to run Agent code.
   b. Press `'d'` to download the agent/diag/bootloader code.
   c. Press `'e'` to display Errors.
   d. Press `'i'` to initialize config flash.
   e. Press `'p'` to run POST tests.
   f. Press `'r'` to reset the switch.
4. Press `'d'`.
5. Choose `option: 2 - Diagnostics`.
6. Choose `option: 1 — Download via TFTP`.
7. Enter the filename, along with its extension; for example `3500_10012_diag.bin`
8. Enter the TFTP server IP address.
9. Enter the switch IP address.
10. Enter the subnet mask.
11. Enter the port in which the cable is connected.
    The download of the DIAG image begins.

Updating the Bootloader image from the Boot menu

Use this procedure to update the Bootloader image from the Boot menu.

Procedure

1. Connect a default switch to a TFTP server.
2. Reboot the switch (either a soft or hard reset).

3. During the boot process, press `CTRL+C` until the following menu is displayed:
   a. Press `'a'` to run Agent code.
   b. Press `'d'` to download the agent/diag/bootloader code.
   c. Press `'e'` to display Errors.
   d. Press `'i'` to initialize config flash.
   e. Press `'p'` to run POST tests.
   f. Press `'r'` to reset the switch.
4. Press `'d'`.
5. Choose `option: 3- Bootloader`.
6. Choose `option: 1 – Download via TFTP`.
7. Enter the filename, along with its extension; for example `ERS3500_b1_0_0_4.bin`
8. Enter the TFTP server IP address.
9. Enter the switch IP address.
10. Enter the subnet mask.
11. Enter the port in which the cable is connected.
    The download of the DIAG image begins.
12. Press `'y'` to program flash when prompted after download.
13. Once the download and programming completes, you can either additionally download the Diags or Agent image, or press `'y'` to reboot the switch.

Supported software and hardware capabilities

The following table summarizes the known capabilities for the Avaya Ethernet Routing Switch 3500 Series software.

Table 4: Supported capabilities for the Avaya Ethernet Routing Switch 3500 Series

Feature	Maximum number supported
QoS egress queues	4
QoS filters per precedence	256
QoS precedence	4
Total QoS filters	(4 x 256) = 1024
MAC addresses	16000

Feature	Maximum number supported
Layer 2	
VLANs	256
Spanning Tree Groups in STPG and RSTP modes	1
Multiple Spanning Tree Instances (MSTI) in MSTP mode	8
MultiLink Trunking (MLT), Link Aggregation (LAG) groups	6
Links for each MLT or LAG	4
Layer 3	
ARP entries (local, static & dynamic)	512 (of which 32 are reserved for local ARPs)
Local ARP Entries (local IP interfaces)	32
Static ARP entries	256
Dynamic ARP entries	max 480 (shares 480 entries with dynamic ARPs)
IPv4 route entries (local, static & dynamic)	32 local + 32 static + 0 dynamic
Static routes and Non-local Static routes	32
Local routes	32
Management routes	4
UDP Forwarding entries	128
DHCP relay entries	256
DHCP relay forward paths	256
DHCP Server Pools	16 (one per VLAN)
DHCP Server clients per pool	256
DHCP Server clients per switch/stack	2000
Miscellaneous	
802.1X EAP scaling (clients for each port)	32
ADAC (IP Phones)	16
Jumbo frame support	9 K bytes
IGMP multicast groups	up to 59
802.1X (EAP) clients per port, running in MHMA	32
802.1X (EAP) clients per switch	384

Feature	Maximum number supported
LLDP Neighbors	160 on ERS 3510GT 416 on ERS 3524GT 448 on ERS 3526T 816 on ERS 3549GTS
RMON alarms	400
RMON events	400
RMON Ethernet statistics	128 per unit
RMON Ethernet history	196 per unit

Supported standards RFCs and MIBs

Standards

The standards in the following list are supported on the switch:

- IEEE 802.1AB (Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discover (LLDP-MED))
- IEEE 802.1Q (VLANs)
- IEEE 802.1p (Priority Queues)
- IEEE 802.1D (Spanning Tree)
- IEEE 802.1w (Rapid Spanning Tree)
- IEEE 802.1s (Multiple Spanning Tree Groups)
- IEEE 802.1X (Extensible Authentication Protocol (EAP))
- IEEE 802.3 (10BASE-T/100BASE-TX)
- IEEE 802.3u (100BASE-T (ANSI) Auto-Negotiation)
- IEEE 802.3x (Pause Frames / Flow Control)
- IEEE 802.3z (1000BASE-X)
- IEEE 802.3ab (1000BASE-T)
- IEEE 802.3ad (Link Aggregation Control Protocol (LACP))
- IEEE 802.3af (Power over Ethernet — PoE (15.4W))

- IEEE 802.3aq (10GBASE-LRM 10 Gbit/s Ethernet over fiber)
- IEEE 802.3at (Power over Ethernet plus— PoE+ (32W))

RFCs and MIBs

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

- RFC 783 Trivial File Transfer Protocol (TFTP)
- RFC 791/ 950 Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 826 Address Resolution Protocol (ARP)
- RFC 854 Telnet Server and Client
- RFC 951/ 1542 (BOOTP)
- RFC 1112 Internet Group Management Protocol v1 (IGMPv1)
- RFC 1213 MIB-II
- RFC 1215 SNMP Traps Definition
- RFC 1271 / 1757 / 2819 RMON
- RFC 1361 / 1769 Simple Network Time Protocol (SNTP)
- RFC 1493 (Bridge MIB)
- RFC 1573 / 2863 Interface MIB
- RFC 1643 / 2665 Ethernet MIB
- RFC 1905 / 3416 SNMP
- RFC 1906 / 3417 SNMP Transport Mappings
- RFC 1907 / 3418 SNMP MIB
- RFC 1945 HTTP v1.0
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2011 SNMP v2 MIB for IP
- RFC 2012 SNMP v2 MIB for TCP
- RFC 2013 SNMP v2 MIB for UDP
- RFC 2131 DHCP Client
- RFC 2132 DHCP Options 6, 43 & 60
- RFC 2138 RADIUS
- RFC 2236 Internet Group Management Protocol v2 (IGMPv2)

- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IPv6
- RFC 2462 Auto-configuration of link local addresses
- RFC 2474 Differentiated Services Support
- RFC 2570 / 3410 SNMPv3
- RFC 2571 / 3411 SNMP Frameworks
- RFC 2572 / 3412 SNMP Message Processing
- RFC 2573 / 3413 SNMPv3 Applications
- RFC 2574 / 3414 SNMPv3 USM
- RFC 2575 / 3415 SNMPv3 VACM
- RFC 2576 / 3584 Co-existence of SNMP v1/v2/v3
- RFC 2616 HTTP
- RFC 2660 HTTPS (Secure Web)
- RFC 2665 Ethernet MIB
- RFC 2674 Q-Bridge MIB
- RFC 2737 Entity MIBv2
- RFC 2819 RMON MIB
- RFC 2863 Interfaces Group MIB
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions (interim updates)
- RFC 3046 (& 5010) DHCP option 82, Relay Agent Information Option
- RFC 3058 RADIUS Authentication
- RFC 3361 DHCP option 120 SIP Servers
- RFC 3376 Internet Group Management Protocol v3 (IGMPv3)
- RFC 3576 RADIUS Change of Authorization
- RFC 4007 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4252 SSH
- RFC 4291 IPv6 Addressing Architecture
- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4432 SSHv2 RSA
- RFC 4443 Internet Control Message Protocol (ICMPv6) Update to RFC 2463

- RFC 4675 RADIUS Attributes for VLAN and Priority Support
- RFC 5859 TFTP Server DHCP option

Chapter 4: Resolved issues

Use the information in this section to learn more about issues that have been resolved in Release 5.2.

Resolved issues in Release 5.2

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

Reference number	Description
wi01034083	**MIB walk, EDM**: Occasionally the walk performed on 1.3 from EDM may fail due to the EDM timeout.
wi01048337	**EDM**: Cannot set eap advance settings for the options that are situated on the last columns. The options situated in the last columns of the EDM cannot be changed for a random port due to the scroll returning automatically to the first columns. As workaround please use the multiple port selection.
wi01049621	**LACP, mrouter**: LACP and mrouter ports are mutual exclusive. It is recommended to use mrouter ports with MLT
wi01059318	**Web/Telnet/Console, EDM**: You can only change the authentication type in Web/Telnet/Console tabs in EDM for a single unit. Resolved with the Unified password feature.
wi01062753	**EDM, DHCP Relay**: There is no DHCP Relay counter in EDM. To show the count, use the ACLI command **`show ip dhcp-relay counter`**.
wi01066463	**Autosave**: The use of the autosave command is not recommended for large stacked environments unless an uninterruptable power supply (UPS) is also present. If the autosave command remains enabled, then configuration information can be lost under several unexpected stack power-down scenarios. The command **`no autosave enable`** should be applied to all stacks lacking a UPS that also have user applied configuration settings (i.e. multiple VLAN). You must then manually save changes every time the configuration is altered (by the user) using the **`save config`** command. The **`no autosave enable`** setting needs to be manually saved using the **`save config`**.
wi01070950 wi01070945	**Platform Stack**: ipAddrTable not correct, two entries instead of one. ipAdEntBcastAddr value not correct.

Reference number	Description
wi01073527	**DHCP Snooping**: After the DHCP Snooping Binding Table is full, DHCP Clients Discovery are not blocked from continuing to receive addresses.
wi01076616	**DHCP Server**: IP host pools do not register the correct host when multiple IP pools are configured on the stack.
wi01079577	**NEAP**: NEAP IP phone appears authenticated as NEAP client with state "Unknown".
wi01079880	**Flow Control**: Setting the flow control of a 1G port to Symmetrical will display the following message although the QoS does not support the lossless mode: "% Flow Control can only be set to Symmetric when QOS agent buffer is set to Lossless mode'.
wi01117718	ERS3500 SW 5.1.0.006 Memory Leak.
wi01152217	Switch unreachable via management VLAN.
wi01152225	Snmpgetnext for ifndex,ifinOctets and ifType returns wrong ifInOctets data.
wi01152230	Syslog error "VLAN NVRAM read error".
wi01152467	High CPU utilization with task "tLAC" taking 67% of the cpu.
wi01152524	SnmpGet shows zeros for port statistics when multiple OIDs are polled.
wi01152530	35xx appears to drop ARP packets on voice VLAN from Avaya SIP phones.
wi01152534	Telnet and HTTP stopped working, reboot required to restore operation.

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.

Known issues in Release 5.2

The following table lists and describes known issues and limitations for Avaya Ethernet Routing Switch 3500 Series Software Release 5.2. Where available and appropriate, workarounds are provided.

Reference number	Description
wi01041815	**Image file download**: If an image checksum is incorrect, the system returns the following message: `% Invalid image`
wi01058803	In EDM, the Mac Violation tab does not display anything. Use show log.

wi01059140	**DHCP Snooping, ACLI**: The following error message may appear when enabling the IP DHCP Snooping per VLAN:
	`% Cannot modify settings`
	`% Error setting VLAN DHCP snooping`

wi01070932 wi01129521 wi01130292 wi01133577	**3526T and 3526T-PWR+, NVR Sw Exception critical logs:** On the ERS3526 models, exceptions with the Unknown type may appear when the power is cut. No actual exceptions occur - the device functionality and its configuration are not affected. This also occurs on soft resets.
wi01079448	**MIB, Temperature sensor:** The Temperature sensor in the 35XX units is currently defined as a "Metro1200ESM"
wi01124460	DHCP Client info is missing from EDM.
wi01124487	**DHCP Client**: Incorrect lease time is received when configuring the DHCP client lease on the DUT and its value is above 3600 seconds.
wi01125690	**Storm Control**: Storm Control Action Drop Enable will not generate an error message unless there are no precedences available at the time it is being set. If a policy is created afterwards and there is no precedence available at the time storm control is triggered, then the function will not work and a log message is generated. Customers should check for one free precedence by using the **`show qos diag`** command.

Reference number	Description
wi01146473	There is a discrepancy between the Diagnostic reset count, which increments every time the software starts Diagnostics, and the **show sys-info** reset count increments when the agent comes all the way up.
wi01146838	**EDM Network Management**: Missing snmp link trap commands. The Link trap was replaced by a link notification trap for both link up and link down and is controlled in the SNMP Notification Control field. The values viewed under the edit port/ports will now be greyed out with Enabled. To see the actual values in EDM the user will need to go to Configuration-> Edit-> SNMP Server-> Notification Control.
wi01151880	Phones are not authenticated by DHCP signature. Workaround: Enable guest VLAN on the ports where the phones are connected and the phones will be authenticated by DHCP.
wi01152177	**ADAC**: Wrong port assignation when using ADAC UFA and certain settings. Avaya recommends the user do not use ADAC and LLDP at the same time with Avaya Phones.
wi01156743	ERS-3526T-PWR+ (5.1.0.006): Running a MIB-Walk on an ERS 35xx (SW v5.1) switch returns a warning for a non-existing Power-Supply.
From Release 5.0	
wi00966215 wi00966455 wi00968425	**Precedence:** The ASIC has only four slices (precedences) for all the ports. All these slices are occupied by default (one used by ARP, two by QoS and one by DHCP). In order to enable Auto QoS/ADAC/IPSG/UDP Fwd, at least one precedence should be freed. The precedences used by QoS can be freed by issuing the following commands: **(config)# qos if-group name <GROUP_NAME> class <trusted | unrestricted | untrustedbasic>** **(config)# qos if-assign port all name <GROUP_NAME>** The precedence used by DHCP can be freed by issuing the following command: **(config)# no ip dhcp-relay** Note that the precedence used by ARP cannot be freed.
wi00988287	**ASCII config file:** There is a difference between ACLI and EDM in how an ASCII config file is executed on all platforms. When encountering an error, EDM stops the execution and the operation fails, whereas ACLI moves to the next command.
wi00988195	**sftp syslog:** Saving the binary configuration to an external TFTP or SFTP server will generate a `bsnConfigurationSavedToNvram` message in the Syslog as the configuration is saved in the NVRAM prior sending it.

Reference number	Description
wi00984443	**Fan Failure:** If an ERS 3510GT-PWR+ fan fails, during diagnostics, the Status LED should flash Amber, but the Power LED lights Amber instead.