



Avaya Ethernet Routing Switch 3500 Series Release Notes

Release 5.1.1
NN47203-400
Issue 03.03
August 2013

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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 its hardware and Software ("Product(s)"). 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>. 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. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED 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 AUTHORIZED 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". 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, or hardware provided by Avaya. All content on this site, the documentation 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 that 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"). 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>. 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>. 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 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 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>.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

| | |
|--|-----------|
| Chapter 1: Introduction | 7 |
| Purpose..... | 7 |
| Chapter 2: New in this release | 9 |
| Features in release 5.1.1..... | 9 |
| Backup CONFIG file..... | 9 |
| Secure SLA Monitor agent-server communication..... | 9 |
| SLA Monitor CLI and EDM Support..... | 10 |
| Features in release 5.1..... | 10 |
| Hardware..... | 11 |
| Features..... | 11 |
| Chapter 3: ERS 3500 5.1.1 Feature Configuration | 17 |
| SLA Monitor configuration..... | 17 |
| Configuring SLA Monitor using ACLI..... | 17 |
| Configuring SLA Monitor using EDM..... | 25 |
| Chapter 4: Important notices | 33 |
| Important notices..... | 33 |
| File names for release 5.1.1..... | 33 |
| File names for release 5.1..... | 34 |
| Upgrading the Diag image using ACLI..... | 35 |
| Updating the Diag image from the Boot menu..... | 36 |
| Updating the Bootloader image from the Boot menu..... | 36 |
| Supported software and hardware capabilities..... | 37 |
| Supported standards RFCs and MIBs..... | 39 |
| Standards..... | 39 |
| RFCs and MIBs..... | 40 |
| Chapter 5: Resolved issues | 43 |
| Resolved issues in Release 5.1.1..... | 43 |
| Resolved issues in Release 5.1..... | 43 |
| Chapter 6: Known issues and limitations | 45 |
| Known issues and limitations..... | 45 |
| Known issues in Release 5.1.1..... | 45 |
| Known issues in Release 5.1..... | 45 |

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 5.1.1.

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 is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

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.

Training

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

Chapter 2: New in this release

The following sections detail what is new in Avaya Ethernet Routing Switch 3500 Series Release 5.1 and Release 5.1.1.

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

Features in release 5.1.1

See the following sections for information about feature changes in release 5.1.1.

Backup CONFIG file

The Backup CONFIG file feature prevents the effects of corruption of the configuration file in the case of a power failure occurring during the process of writing the configuration to NVRAM, through the creation of an automatic backup configuration file. When the switch boots, if it detects a corrupted primary configuration, the switch automatically loads the backup configuration file and generates an appropriate log entry.

Secure SLA Monitor agent-server communication

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 agent23 server communications.

Note:

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

SLA Monitor CLI and EDM Support

SLA Monitor uses two types of tests to determine QoS benchmarks:

- Real Time Protocol (RTP)

This test measures network performance, for example, jitter, delay, and loss, by injecting a short stream of UDP packets from source to destination (an SLA Monitor agent).

- New Trace Route (NTR)

This test is similar to traceroute but also includes DSCP values at each hop in the path from the source to the destination. The destination does not need to be an SLA Monitor agent.

You can use NTR and RTP tests in the absence of Avaya Diagnostic Server. Following tests can be performed in the absence of Avaya Diagnostic Server:

- You can access the SLA Monitor CLI interface through the SLAMon Agent Address SLAMon Agent Port. By default, the access to the SLA Monitor CLI interface is disabled. If access is enabled, the SLA Monitor CLI interface becomes available when the SLA Monitor agent is enabled. Tests are run serially and only one type of test can be run at a time. Established sessions time-out after a specified interval. The time interval can be 60 seconds to 600 seconds. By default, the interval is 60 seconds and 0 indicates time-out or disabled. You can disable the SLA Monitor CLI interface if the functionality is not required.
- You can run the NTR and RTP tests through the ACLI using the Application Configuration mode. The SLA Monitor agent must be enabled. Tests are run serially and only one type of test can be run at a time.

Error message “Unable to initiate test - agent busy” or “Reported Issue: test request denied by remote agent” appears if any tests are executed during the same time when the tests initiated by the server are executed. The server initiated tests are executed on priority. Do any one of the following if the error message appears:

- Stop the server
- Enable SLAMon Agent Refuse Server Tests on the remote agent

Note:

Command execution fails if you disable the SLA Monitor agent.

Features in release 5.1

See the following sections for information about feature changes in release 5.1

Hardware

The following table lists and describes the hardware that is new for the Avaya Ethernet Routing Switch 3500 Series Release 5.1:

Table 1: Hardware

| Hardware | Description |
|---------------------|---------------------------|
| Stack cables | |
| AL3518001–E6 | ERS 3500 46cm Stack Cable |
| AL3518002–E6 | ERS 3500 1.5m Stack Cable |
| AL3518003–E6 | ERS 3500 3m Stack Cable |

Features

The following sections highlight the feature support provided in Release 5.1.

802.1X EAP Separate enable/disable

This feature allows both EAP/NEAP client types on the same port as distinct configuration options and with independent functionalities provided for each client type.

In Release 5.0, when EAP was enabled on a port by setting the port admin status to auto, EAP clients were allowed on the port, but NEAP clients were not allowed on the port. The per port option “allow-non-eap-enable” was required to enable the NEAP clients. In Release 5.1, new global and per-port configuration options have been added which allow EAP to be enabled globally (default), and then choose to enable and/or disable EAP and NEAP clients on a port basis, or have no client types enabled on a port.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Security (NN47203–504)*.

802.1X EAP and NEAP Accounting

In Release 5.0 RADIUS Accounting supports switch login events and EAP authentication, with RADIUS Interim Updates being supported for EAP clients. In Release 5.1 Accounting support is extended to generate accounting messages and interim updates for EAP and Non-EAP (NEAP) clients.

If a NEAP IP Phone is enabled, which authenticated a heritage Nortel IP Phone via its DHCP signature, then such authentication results in accounting messages being generated.

If different servers are configured for EAP/NEAP servers then the accounting messages go to the respective servers.

No additional CLI, MIB or EDM configuration is required for this feature; NEAP accounting is enabled when RADIUS accounting is enabled.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Security* (NN47203–504).

Agent Auto Unit Replacement (AAUR)

As part of Auto Unit Replacement functionality, Agent Auto Unit Replacement (AAUR), is used to ensure that all units in a stack have the same software image by inspecting units joining a stack and downloading the stack software agent image to any unit that has a dissimilar image. AAUR is enabled by default. For more information, see *Avaya Ethernet Routing Switch 3500 Series Getting Started* (NN47203–301).

Auto Unit Replacement (AUR)

The Auto Unit Replacement (AUR) feature enables users to replace a unit from a stack while retaining the configuration of the unit. This feature requires the switch stack to remain powered on during the unit replacement.

The main feature of AUR is the ability to retain the configuration (CFG) image of a unit in a stack during a replacement of a failed unit in the stack. The CFG image from the old unit is restored to the new unit. Because retained CFG images are kept in the DRAM of the stack, the stack power must be kept on during the procedure.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Getting Started* (NN47203–301).

Diagnostics Auto Unit Replacement (DAUR)

As part of Auto Unit Replacement functionality, Diagnostic Auto Unit Replacement (DAUR) is used to update the diagnostic image on a non-base unit with the diagnostic image saved in the base unit of a switch stack, if the images differ. When you enable or disable Agent Auto Unit Replacement (AAUR), you automatically enable or disable DAUR in conjunction with AAUR. The default setting for AAUR and DAUR is enabled. For more information, see *Avaya Ethernet Routing Switch 3500 Series Getting Started* (NN47203–301).

DHCP Server

If you require local provision of TCP/IP addresses and have no separate Dynamic Host Configuration Protocol (DHCP) Server or other device available to provide the service to local hosts, a DHCP Server is included and embedded on the switch. You can use the DHCP Server feature to provide and manage client IPv4 addresses in your network and eliminate manual TCP/IP configuration. The DHCP Server is disabled by default.

Ethernet Routing Switch 3500 Series Release 5.1 provides support for DHCP Server Option 241 and 242, as well as the ability to view DHCP Server leases in EDM. For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — IP Routing and Multicast* (NN47203–502).

Distributed LAG (802.3ad LACP)

Distributed Link Aggregation Group (D-LAG) supports up to six link aggregation trunk groups with a maximum of four active members per group using the Link Aggregation Control Protocol (LACP) over point-to-point links in each group. Link members can be ports from a local unit or from any other unit in a switch stack. For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — Layer 2* (NN47203–500).

Distributed MLT (DMLT)

Distributed Multi-Link Trunking (DMLT) supports up to six link aggregation trunk groups with a maximum of four members per group using either a basic or advanced load balancing algorithm. Link members can be ports from a local unit or from any other unit in a switch stack. For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — Layer 2* (NN47203–500).

Identify Units (Blink LEDs)

With the `blink-1eds` command, you can set the LEDs on the display panel of each ERS 3500 Switch to blink to identify a particular unit in a switch stack.

Following a reset or power up, if the switch detects power on its stacking cables and is connected to another unit, the switch shuts down all its local ports. When the ports are disabled, the port LEDs blink, similar to ports that are shut down. The ports are reenabled when the unit finishes entering the stack formation or after a 60-second timeout, whichever comes first.

If the unit does not detect power on the stacking ports in 20 seconds after it comes up, ports forward the traffic.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Getting Started* (NN47203–301).

IP blocking

IP blocking is a feature of the Avaya Ethernet Routing Switch 3500 Series, that provides safeguards for a stack where VLANs enabled with an IP address and Layer 3 forwarding contain port members across multiple stack units. IP blocking is used whenever a unit leaves a stack or is rebooting inside the context of a stack. Depending on the setting in use, Layer 3 functionality is either continued or blocked by this feature.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — IP Routing and Multicast* (NN47203–502).

LLDP configurable MED network policy (5.0.1)

You can configure 802.1AB MED network policies to dynamically configure voice VLAN, DSCP, priority, and VLAN tagging on the switch for voice traffic received from an IP phone. When you enable LLDP and configure the MED network policies on the switch, the switch sends the network policies to the IP Phone. The IP phone processes the data in the LLDP PDU and transmits the voice traffic with the appropriate VLAN ID, VLAN tagging, DSCP and priority information.

You can configure MED network policies on a switch port that has ADAC enabled. The network policies have priority over the ADAC configuration on the port.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — Layer 2* (NN47203–500).

Run IP Office Script (5.0.1)

This feature introduces an ACLI script that configures parameters for the ERS3500 switch according to Avaya best practices for converged solutions. The script can be executed in automatic mode where the configuration set with pre-determined parameters or in verbose mode where the installer can enter parameters when prompted by ACLI. The script configuration setup is optimized for solutions with IP Office supporting approximately 2 to 22

users, so that a technician can quickly and easily set up an ERS3500 switch in a best practices solution with Avaya IP Office. In Release 5.1 with stacking support, the script can now support up to 192 switch ports. The script sets VLAN IDs, IP addresses, QoS rules and tagging modes on switch ports to specific values and PoE priorities for PWR units. LLDP for IP Phone detection is set automatically and switch ports are configured to which the IP Office call server can connect. The script executes the set of CLI commands using the ACLI command `run ipoffice` (fully automated configuration), or `run ipoffice verbose` (user prompted configuration). The script settings can be displayed using the `show running-config` command. The script is available in both standalone and stacking mode. In stacking mode, you must execute the script from the Base Unit.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Getting Started* (NN47203–301).

Service Level Agreement (SLA) Monitor (5.0.2)

Release 5.1 adds support for the SLA Monitor agent. You can use SLA Monitor to monitor and analyze performance issues in the network infrastructure.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — System Monitoring* (NN47203–501).

Show UTC Timestamp (5.0.2)

The show UTC timestamp feature enables you to display the UTC timestamp after issuing any show command in ACLI. By default, the timestamp state is disabled.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Getting Started* (NN47203–301).

Stack Forced Mode

Stack Forced Mode primarily provides management IP continuity of a two-unit stack if one unit fails in the stack. This extends to a two-unit stack that may both become stand-alone switches if the stacking mechanism between both units fails. You can manage the units from the broken stack in Stack Forced Mode, depending on the location of uplink(s). If you enable Stack Forced Mode on a stack, you enable Stack Forced Mode on both units in the two-unit stack. Stack Forced Mode becomes active only if the stack fails. For more information, see *Avaya Ethernet Routing Switch 3500 Series Getting Started* (NN47203–301).

Stack Health Check

The Stack Health Check feature provides at-a-glance information of the stacking state on rear cascade ports of each switch. It is used to run a test to monitor the rear cascade port status for each unit, confirm the number of switching units in stack, detect if a cable is broken or missing, detect if the stack is operating with a temporary base unit, and to summarize the stack operational health. For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — System Monitoring* (NN47203–501).

Stack IP Address

You can assign an IP Address to the base unit switch in a switch stack using ACLI. For more information, see *Avaya Ethernet Routing Switch 3500 Series Getting Started* (NN47203–301).

Stack Monitor & Statistics

The Stack Monitor uses a set of control values to enable its operation, to set the expected stack size, and to control the frequency of trap sending. The stack monitor, if enabled, detects problems with the units in the stack and sends a trap.

The Stack monitor sends a trap for the following events.

- The number of units in a stack changes.
- The trap sending timer expires.

Each time the number of units in a stack changes, the trap sending timer resets and the stack monitor compares the current number of stack units with the configured number of stack units. If the values are not equal, the switch sends a trap and logs a message to syslog. The stack monitor sends traps from a stand-alone unit or the base unit of the stack.

After the trap sending timer reaches the configured number of seconds at which traps are sent, the switch sends a trap and logs a message to syslog and restarts the trap sending timer. The syslog message is not repeated unless the stack configuration changes.

After you enable the stack monitor on a stack, the stack monitor captures the current stack size and uses it as the expected stack size. You can choose a different value and set it after you enable the feature.

In Release 5.1, the Avaya ERS 3500 series switch also enables the viewing of diagnostic and statistical information. For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — System Monitoring* (NN47203–501).

Storm Control

This feature provides granular control of Broadcast, Multicast and Unicast traffic rates on a per-port basis. Broadcast, Multicast and Unicast traffic rates can be individually or collectively controlled on a switch or switch stack by setting the following: low-watermark and high watermark values in packets per second (pps), polling interval value, action type, and SNMP traps. When a high-watermark is exceeded, an action of None, Drop or Shutdown can be applied to the traffic type.

A defined action is reversed, or ceases, when the traffic rate in pps falls below the low-watermark setting. When an action of 'drop' is used, traffic is dropped when traffic exceeds the high-watermark and will not resume forwarding until the traffic rate falls below the low-watermark. When the action of 'shutdown' is used, the switch port is administratively shutdown when traffic exceeds the high-watermark and requires administrator intervention to re-enable the switch port to resume traffic forwarding.

The Storm Control feature includes logging of watermark crossings and sending of traps for the low and high watermark crossings. Traps for high watermark exceeded may be sent repeatedly at a user specified interval. For more information, see *Avaya Ethernet Routing Switch 3500 Series Security* (NN47203–504).

Unit Stack Uptime

The Avaya ERS 3500 series switch displays the stack uptime for each unit in a stack and reports when requested.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — System Monitoring* (NN47203–501).

Voice VLAN Integration

Voice VLAN Integration provides centralized creation and management of up to 6 voice VLANs using VLAN-specific commands. With Voice VLAN Integration, each application (e.g. ADAC or EAP) will use these voice VLANs. For ADAC this means you must configure a VLAN as Voice type and be present on the switch before you can configure the ADAC to use that VLAN. As the ADAC VLAN is no longer dynamic, this brings additional benefits in that VLAN membership and configuration can be customized and retained across reboots and that if required, Layer 3 can also be enabled on the ADAC VLAN.

For more information, see *Avaya Ethernet Routing Switch 3500 Series Configuration — Layer 2* (NN47203–500).

Other changes

Enterprise Device Manager (EDM) enhancements

In Release 5.1 the navigation tree in EDM has the following changes:

- **Serviceability folder** - the Rmon folder now resides under this new Serviceability folder under Configuration. SLA Monitor can also be found under the Serviceability folder.
- **Help folder** - additional information can be found under the Help folder, which includes a Legend folder with port status and color meanings

Chapter 3: ERS 3500 5.1.1 Feature Configuration

This chapter contains information about Release 5.1.1 features.

SLA Monitor configuration

You must enable the SLA Monitor agent to run specific QoS tests in the absence of an Avaya Diagnostic server. Agents exchange packets between one another to conduct the QoS tests. SLA Monitor uses Real Time Protocol (RTP) and New Trace Route (NTR) tests to determine QoS benchmarks.

Note:

SLA Monitor agent communications are IPv4-based. Agent communications do not currently support IPv6.

Configuring SLA Monitor using ACLI

Use the procedures in this section to configure the SLA Monitor agent.

Displaying SLA Monitor agent settings

Use this procedure to view the global SLA Monitor agent settings.

Procedure

1. Enter Privileged EXEC command mode in ACLI.
2. At the command prompt, enter the following command:
`show application slamon agent`

Example

```
3510GT-PWR+>enable
3510GT-PWR+#show application slamon agent
SLAMon Operational Mode: Enabled
SLAMon Agent Encryption: Not Supported
SLAMon Agent Address: 172.16.120.10
```

```

SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Not Registered
SLAMon Registered Server Address: 0.0.0.0
SLAMon Registered Server Port: 0
SLAMon Server Registration Time: 0
SLAMon CLI Mode: Enabled
SLAMon CLI Timeout Mode: Enabled
SLAMon CLI Timeout: 60 seconds
SLAMon Configured Agent Address: 0.0.0.0
SLAMon Configured Agent Port: 0
SLAMon Configured Server Address: 0.0.0.0 0.0.0.0
SLAMon Configured Server Port: 0
SLAMon Agent-To-Agent Communication Port: 50012
SLAMon Configured Agent-To-Agent Communication Port: 0
SLAMon Agent Server Bypass: Disabled
SLAMon Agent Refuse Server Tests: Allow Tests

```

Configuring SLA Monitor using ACLI

Use this procedure to configure the SLA Monitor agent to perform Quality of Service (QoS) tests of the network.

Before you begin

To take full advantage of the SLA Monitor agent, you must have an Avaya Diagnostic server in your network. You can perform the Quality of Service (QoS) tests without a server.

About this task

To configure the agent, you must enable the agent and assign an IP address. By default, the agent uses the switch/stack IP address if a specific agent address is not configured. Remaining agent parameters are optional and you can operate the agent using the default values.

Procedure

1. Enter Application Configuration mode in ACLI.
2. To configure the agent IP address, enter the following command:
`slamon agent ip address {A.B.C.D}`
3. To configure the agent IP address to its default value, enter the following command:
`default slamon agent ip address`
4. To configure the UDP port, enter the following command:
`slamon agent port <0-65535>`
5. To configure the agent UDP port to its default value, enter the following command:
`default slamon agent port`
6. To enable the agent, enter the following command:
`slamon oper-mode enable`
7. To disable the agent, enter the following command:
`no slamon oper-mode [enable]`

OR

```
default slamon oper-mode
```

8. To configure the agent-to-agent communication port, enter the following command:

```
slamon agent-comm-port <0-65535>
```

9. To configure the agent-to-agent communication port to its default value, enter the following command:

```
default slamon agent-comm-port
```

10. To enable the SLA Monitor agent CLI support, enter the following command:

```
slamon cli enable
```

Note:

The CLI commands affect only the SLA Monitor (SLM) CLI commands and not the standard platform CLI commands.

11. To disable the SLA Monitor agent CLI support, enter the following command:

```
no slamon cli [enable]
```

OR

```
default slamon cli
```

12. To configure the agent automatic CLI session timeout value, enter the following command:

```
[default] slamon cli-timeout <60-600>
```

13. To enable the agent automatic CLI session timeout, enter the following command:

```
slamon cli-timeout-mode enable
```

OR

```
default slamon cli-timeout-mode
```

14. To disable the agent automatic CLI session timeout, enter the following command:

```
no slamon cli-timeout-mode [enable]
```

15. To configure the agent server IP address, enter the following command:

```
slamon server ip address {A.B.C.D} [{A.B.C.D}]
```

16. To configure the agent server IP address to its default value, enter the following command:

```
default slamon server ip address
```

17. To configure the server TCP registration port, enter the following command:

```
slamon server port <0-65535>
```

18. To configure the server TCP registration port to its default value, enter the following command:

```
default slamon server port
```

19. To enable the agent refuse server test mode, enter the following command:

```
slamon refuse-server-tests [enable]
```

20. To disable the agent refuse server test mode, enter the following command:

```
no slamon refuse-server-tests [enable]
```

OR

```
default slamon refuse-server-tests
```
21. To enable the agent server bypass mode, enter the following command:

```
slamon server-bypass [enable]
```
22. To disable the agent server bypass mode, enter the following command:

```
no slamon server-bypass [enable]
```

OR

```
default slamon server-bypass
```
23. To display the SLA monitor configuration, enter the following command:

```
show application slamon agent
```

Example

```
3510GT-PWR+>enable
3510GT-PWR+#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3510GT-PWR+(config)#application
3510GT-PWR+(config-app)#slamon oper-mode enable
3510GT-PWR+(config-app)#show application slamon agent
SLAMon Operational Mode: Enabled
SLAMon Agent Encryption: Not Supported
SLAMon Agent Address: 172.16.120.10
SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Not Registered
SLAMon Registered Server Address: 0.0.0.0
SLAMon Registered Server Port: 0
SLAMon Server Registration Time: 0
SLAMon CLI Mode: Enabled
SLAMon CLI Timeout Mode: Enabled
SLAMon CLI Timeout: 60 seconds
SLAMon Configured Agent Address: 0.0.0.0
SLAMon Configured Agent Port: 0
SLAMon Configured Server Address: 0.0.0.0 0.0.0.0
SLAMon Configured Server Port: 0
SLAMon Agent-To-Agent Communication Port: 50012
SLAMon Configured Agent-To-Agent Communication Port: 0
SLAMon Agent Server Bypass: Disabled
SLAMon Agent Refuse Agent Server Tests: Refuse Tests
3510GT-PWR+(config-app)#
```

Next steps

If you have configured SLA Monitor but the agent is not functioning as expected, determine task status using the engineering menu.

If the agent is not in the expected state, reset the system to start the agent.

If the agent task functions as expected, perform typical troubleshooting steps to verify agent accessibility:

- Verify IP address assignment and port use.
- Verify that the SLA Monitor agent is enabled.
- Ping the Avaya Diagnostic server IP address.
- Verify the Avaya Diagnostic server configuration.

Variable definitions

The following table describes the parameters for the `slamon` command.

| Variable | Value |
|----------------------------|--|
| agent | Configures the SLA Monitor agent. |
| agent-comm-port <0–65535> | Configures the SLA Monitor agent-to-agent communication UDP port. |
| agent ip address <A.B.C.D> | Configures the agent IP address. If no IP address is specified, the default value is 0.0.0.0, which causes the agent to use the switch/stack IP address. |
| agent port <0–65535> | Configures the UDP port for agent-server communication. The agent receives discovery packets on this port. The default is port 50011. The server must use the same port. |
| cli | Configures the SLA Monitor agent CLI interface. |
| cli-timeout <60–600> | Configures the CLI timeout value in seconds. The default is 60 seconds. Note: The CLI commands only impact the SLA Monitor CLI and not the standard platform CLI. |
| ntr | Initiates the SLA Monitor NTR test. |
| oper-mode | Disables the SLA Monitor agent. |
| oper-mode enable | Enables the SLA Monitor agent. The default is disabled. If you disable the agent, it does not respond to discover packets from a server. If you disable the agent because of resource concerns, consider changing the server configuration instead, to alter the test frequency or duration, or the number of targets. |

| Variable | Value |
|---|---|
| server ip address {A.B.C.D} [{A.B.C.D}] | Restricts the agent to use of this server IP address only. The default is 0.0.0.0, which means the agent can register with any server. You can specify a secondary server as well. |
| server port <0–65535> | Restricts the agent to use of this registration port only. The default is 0, which means the agent disregards the source port information in server traffic. The server must use the same port. |
| rtp | Initiates the SLA Monitor RTP test. |
| refuse-server-tests | Agent accepts NTR and RTP test requests from the server. |
| refuse-server-tests enable | Agent rejects NTR and RTP test requests from the server. If you disable this mode, the agent accepts test requests from the server with which it is registered. Test requests originating from platform, SLM CLI interfaces, and SNMP are not affected. |
| server | Configures the SLA Monitor server. |
| server-bypass | Disables the SLA Monitor agent server bypass mode. |
| server-bypass enable | Allows an enabled agent to always accept agent-to-agent traffic. When enabled a small number of network ports remain open to process network traffic. You must take this into account if security concerns are high. |

Execute new trace route test using ACLI

Use this procedure to execute a new trace route (NTR) test on the network to establish the Quality of Service (QoS) benchmarks.

Before you begin

To execute the NTR test, you must enable the agent and assign an IP address.

Procedure

1. Enter Application Configuration mode in ACLI.

2. To execute the NTR test, enter the following command:

```
slamon ntr {A.B.C.D} <0-63>
```

Example

```
3510GT-PWR+>enable
3510GT-PWR+#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3510GT-PWR+(config)#application
3510GT-PWR+(config-app)#slamon oper-mode enable
3510GT-PWR+(config-app)#slamon ntr 10.30.56.100 46
```

SLAMon Network Trace Report

```
Source IP/Port: 10.30.56.193:50013
Source DSCP Marking: 46
Destination IP/Port: 10.30.56.100:33434
Maximum TTL: 1
Request Result: OK (Port unreachable)
```

| IP Address | Ingress | Egress | RTT (ms) |
|--------------|---------|--------|----------|
| | DSCP | DSCP | |
| 10.30.56.193 | 46 | 0 | 0.000 |
| 10.30.56.100 | 0 | 0 | 1.240 |

```
3510GT-PWR+(config-app)#
```

Variable definitions

The following table describes the parameters for the `slamon ntr` command.

| Variable | Value |
|------------------------|--|
| IPv4 Address <A.B.C.D> | Specifies the destination IP address. If no IP address is specified, the test execution fails. |
| DSCP <0-63> | Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the NTR test. |
| attempts <1-10> | Specifies the number of attempts generated by the NTR test. The default value is 2. |
| period <1000-200000> | Specifies the interval between packets in microseconds, generated by the NTR test. The default interval is 20000 microseconds. |

Execute real time protocol test using ACLI

Use this procedure to execute a real time protocol (RTP) test on the network to establish the Quality of Service (QoS) benchmark.

Before you begin

To execute the RTP test, you must enable the agent and assign an IP address.

Note:

You must enable the SLA Monitor agent server bypass mode for the RTP test to complete successfully.

Procedure

1. Enter Application Configuration mode in ACLI.
2. To execute the RPT test, enter the following command::

```
slamon RTP {A.B.C.D} <0-63>
```

Example

```
3510GT-PWR+>enable
3510GT-PWR+#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3510GT-PWR+(config)#application
3510GT-PWR+(config-app)#slamon oper-mode enable
3510GT-PWR+(config-app)#slamon rtp 10.30.56.100 46
```

```
-----
SLAMon Real Time Protocol Network Report
-----
```

```
Source IP/Port: 10.30.56.193:50012
Source DSCP Marking: 46
Destination IP/Port: 10.30.56.100:50012
```

```
Delay (RTT): average 1.824 (ms) median 1.701 (ms)
Packet Loss: 0
```

```
Out-of-Order Arrivals:0
```

```
-----
Network Jitter - Quartiles (ms)
-----
```

| 0 | 1 | 2 | 3 | 4 |
|-------|-------|-------|-------|-------|
| 0.007 | 0.173 | 0.208 | 0.224 | 1.343 |

```
-----
3510GT-PWR+(config-app)#
```

Variable definitions

The following table describes the parameters for the `slamon rtp` command.

| Variable | Value |
|------------------------|--|
| IPv4 Address <A.B.C.D> | Specifies the destination IP address. If no IP address is specified, the test execution fails. |
| DSCP <0–63> | Specifies the differential services code point (DSCP) value for use in packets that are generated by the RTP test. |
| npack <10–100> | Specifies the RTP npack value. The default value is 50. |
| nsync <10–100> | Specifies the RTP nsync value. The default value is 10. |
| period <1000–200000> | Specifies the interval between packets in microseconds, generated by the RTP test. The default interval is 20000 microseconds. |

Configuring SLA Monitor using EDM

Use this procedure to configure SLA Monitor.

Procedure

1. In the navigation tree, double-click **Serviceability**.
 2. In the Serviceability tree, click **SLA Monitor**.
 3. In the **SLA Monitor** tab, configure parameters as required.
 4. On the toolbar, click **Apply**.
-

SLA Monitor tab field descriptions

| Name | Description |
|---------------|---|
| Status | <p>Enables or disables the SLA Monitor agent. The default is disabled.</p> <ul style="list-style-type: none"> • enabled: enables the SLA Monitor agent • disabled: disables the SLA Monitor agent |

| Name | Description |
|-----------------------------------|---|
| | <p>If you disable the agent, it does not respond to discover packets from a server.</p> <p>If you disable the agent because of resource concerns, consider changing the server configuration instead, to alter the test frequency or duration, or the number of targets.</p> |
| ServerBypass | <p>Enables or disables the SLA Monitor agent server bypass mode.</p> <ul style="list-style-type: none"> • enabled: enables the SLA Monitor agent server bypass mode. • disabled: disables the SLA Monitor agent server bypass mode. |
| RefuseServerTests | <p>Enables or disables the NTR and RTP test requests from the server.</p> <ul style="list-style-type: none"> • enabled: the SLA Monitor agent rejects test requests from the server with which it is registered. • disabled: the SLA Monitor agent server accepts test requests from the server with which it is registered. <p>Test requests originating from platform, SLM CLI interfaces, and SNMP are not affected.</p> |
| ConfiguredAgentToAgentPort | <p>Specifies the UDP port utilized by the SLA Monitor agent for agent-agent communication. If the value of this attribute is zero, the SLA Monitor agent utilizes a default port value for the base agent-agent UDP communication port.</p> |
| ConfiguredAgentAddrType | <p>Indicates IPv4-based communications.</p> |
| ConfiguredAgentAddr | <p>Specifies the agent IP address. The default value is 0.0.0.0, which causes the agent to use the switch/stack IP address.</p> |
| ConfiguredAgentPort | <p>Specifies the UDP port for agent-server communication. The agent receives discovery packets on this port. The default is port 50011.</p> <p>The server must use the same port.</p> |
| CliAvailable | <p>Specifies whether SLA Monitor agent CLI is available or not available.</p> |
| CliTimeout | <p>Configures the CLI timeout value in seconds. The default is 60 seconds.</p> |

| Name | Description |
|------------------------------------|---|
| CliTimeoutMode | Specifies the maximum amount of time, in seconds, until the CLI session is automatically terminated. The value of this attribute is pertinent only if CLI time-outs are enabled. The default is 60 seconds. |
| ConfiguredServerAddrType | Indicates IPv4-based communications. |
| ConfiguredServerAddr | Specifies the server IP address. If an IP address is specified, the agent is restricted to use this server IP address. The default is 0.0.0.0, which allows the agent to register with any server. |
| ConfiguredServerPort | Specifies the server port. The default is 0, which allows the agent to disregard the source port information in server traffic. The server must use the same port. |
| ConfiguredAltServerAddrType | Indicates IPv4-based communications. |
| ConfiguredAltServerAddr | Specifies a secondary server IP address. |
| SupportApps | Indicates SLA Monitor supported applications. This is a read-only field. |
| AgentAddressType | Indicates IPv4-based communications. This is a read-only field. |
| AgentAddress | Indicates the agent IP address. This is a read-only field. |
| AgentPort | Indicates the agent port. This is a read-only field. |
| RegisteredWithServer | Indicates whether the agent is registered with a server. This is a read-only field. |
| RegisteredServerAddrType | Indicates IPv4-based communications. This is a read-only field. |
| RegisteredServerAddr | Indicates IP address of the SLA Monitor server with which the agent is registered. This is a read-only field. |
| RegisteredServerPort | Indicates the TCP port used by the SLA Monitor server with which the agent is registered. This is a read-only field. |
| RegistrationTime | Indicates the time in seconds, since the agent registered with the server. This is a read-only field. |
| AgentToAgentPort | Indicates the base UDP port used by the SLA Monitor agent for agent-to-agent |

| Name | Description |
|--------------------------|---|
| | communication. The base UDP port is used to derive multiple agent communication ports. This is a read-only field. |
| EncryptionSupport | Indicates if encrypted agent-server communication is supported. |

Executing new trace route test using EDM

Use this procedure to execute new trace route (NTR) test on the network to establish Quality of Service (QoS) benchmark.

Important:

When executing the script using EDM, do not run other commands while the script is in progress, because this slows down the execution. EDM can time-out while waiting for a response and even when a time-out occurs, the script execution continues on EDM.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **SLA Monitor**.
3. In the SLA Monitor work area, click **NTR**.
4. In the NTR work area, click **Insert** to enter parameters for the new test.
5. In the **OwnerId** dialog box, type the owner id.
6. In the **TestName** dialog box, type the test name.
7. In the **TargetAddress** dialog box, type the target IP address.
8. In the **Dscp** dialog box, type the dscp value (0-63).
9. In the **Attempts** dialog box, type the number of attempts (1-10).
10. In the **Period** dialog box, type the type the duration in microseconds (10000–200000).
11. In the **Label** dialog box, type the label.
12. Click **enabled** to enable the administrator status.
13. Click **Insert** to initiate the NTR test.
14. In the NTR work area, click **Results** to view the test results.

Variable Definition

| Variable | Value |
|----------|-------------------------------------|
| OwnerId | Specifies the owner of an NTR test. |

| Variable | Value |
|---------------|---|
| TestName | Specifies the name of an NTR test. |
| TargetAddress | Specifies the target IP address for the NTR test. |
| Dscp | Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the NTR test. |
| Attempts | Specifies the number of attempts generated by the NTR test. The default value is 2. |
| Period | Specifies the interval between packets in microseconds, generated by the NTR test. The default interval is 20000 microseconds. |
| Label | Specifies the text label used to reference the NTR control entry. |
| AdminStatus | Specifies the administrator status. You must enable the administrator status to initiate the NTR test. The administrator status is disabled by default. |

Viewing new trace route test results

Use this procedure to view the new trace route (NTR) test results.

Before you begin

You must execute the NTR test before you view the results.

Procedure

1. In the navigation tree, double-click **Serviceability** .
2. In the Serviceability tree, click **SLA Monitor** .
3. In the SLA Monitor work area, click **NTR** .
4. In the NTR work area, click to select the saved test and then click **Results** .
5. In the results work area, click **NTR Results** to view the NTR test results.

NTR Results tab field descriptions

| Name | Description |
|-------------------|---|
| HopIndex | Indicates the hop index for an NTR test hop. |
| TgtAddress | Indicates the IP address associated with the NTR test hop. |
| Rtt | Indicates the round-trip-time of an NTR test in milliseconds. |

| Name | Description |
|--------------------|---|
| IngressDscp | Indicates the Differential Services Code Point (DSCP) value in the NTR test packet received by the end station for the specified hop. |
| EgressDscp | Indicates the Differential Services Code Point (DSCP) value in the NTR test packet received by the SLA Monitor agent for the specified hop. |

Executing real time protocol test using EDM

Use this procedure to execute real time protocol (RTP) test on the network to establish Quality of Service (QoS) benchmark.

Important:

When executing the script using EDM, do not run other commands while the script is in progress, because this slows down the execution. EDM can time-out while waiting for a response and even when a time-out occurs, the script execution continues on EDM.

Note:

You must enable the SLA Monitor agent server bypass mode for the RTP test to complete successfully.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **SLA Monitor**.
3. In the SLA Monitor work area, click **RTP**.
4. In the RTP work area, click **Insert** to enter parameters for the new test.
5. In the **OwnerId** dialog box, type the owner id.
6. In the **TestName** dialog box, enter the test name.
7. In the **TargetAddress** dialog box, type the target IP address.
8. In the **Dscp** dialog box, type the dscp value (0–63).
9. In the **TestPackets** dialog box, type the number of test packets (10–100).
10. In the **SyncPackets** dialog box, type the number of synchronization packets (10–100).
11. In the **Period** dialog box, type the type the duration in microseconds (10000–200000).
12. Click **enabled** to enable the administrator status.

13. In the **Label** dialog box, type the label.
14. Click **Insert** to initiate the RTP test.
15. In the RTP work area, click **Results** to view the test results.

Variable Definition

| Variable | Value |
|---------------|---|
| OwnerId | Specifies the owner of an RTP test. |
| TestName | Specifies the name of an RTP test. |
| TargetAddress | Specifies the target IP address for the RTP test. |
| Dscp | Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the RTP test. |
| TestPackets | Specifies the number of test packets generated by the RTP test. Test packets are used to determine jitter. |
| SyncPackets | Specifies the number of synchronization packets generated by the RTP test. Synchronization packets are used to determine network delay. |
| Period | Specifies the interval between packets in microseconds, generated by the RTP test. The default interval is 20000 microseconds. |
| Label | Specifies the text label used to reference the RTP control entry. |
| AdminStatus | Specifies the administrator status. You must enable the administrator status to initiate the RTP test. The administrator status is disabled by default. |

Viewing real time protocol test results

Use this procedure to view the real time protocol (RTP) test results.

Before you begin

You must execute the RTP test before you view the results.

Procedure

1. In the navigation tree, double-click **Serviceability** .
2. In the Serviceability tree, click **SLA Monitor** .
3. In the SLA Monitor work area, click **RTP** .
4. In the RTP work area, click to select the saved test and then click **Results** to view the RTP test results.

RTP Results tab field descriptions

| Name | Description |
|--|---|
| OperStatus | Indicates the status of an RTP test. <ul style="list-style-type: none"> • inProgress indicates that an RTP test is in progress. • aborted indicates that an RTP test is aborted. • completed indicates that an RTP test is completed. |
| SrcAddress | Indicates the source IP address used for the RTP test. |
| SrcPort | Indicates the port used for the RTP test. |
| DstAddress | Indicates the destination IP address used for the RTP test. |
| DstPort | Indicates the destination port used for the RTP test. |
| Dscp | Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the RTP test. |
| AverageDelay | Indicates the average network delay (RTT) experienced during the RTP test execution in microseconds. |
| MedianDelay | Indicates the median network delay experienced during an RTP test execution in microseconds. |
| PacketLoss | Indicates the count of packets lost during an RTP test execution. |
| OutOfOrderArrivals | Indicates the count of packets arriving out-of-order during an RTP test execution. |
| JitterQuartile0 – JitterQuartile5 | Indicates the resulting quartile boundaries after sorting the network jitter values of all test packets during an RTP test execution. The value is represented in microseconds |
| AbortData | Indicates the details of the RTP test that was aborted. |

Chapter 4: Important notices

Important notices

This section provides important software and hardware related notices.

File names for release 5.1.1

The following table describes the Avaya Ethernet Routing Switch 3500 Series, Software Release 5.1.1, software files. File sizes are approximate.

| Module or file type | Description | File name | File size (bytes) |
|---|---|---|-------------------|
| Standard (non-SSH) runtime image software version 5.1.1 | Standard software image for the Avaya Ethernet Routing Switch 3500 Series | 3500_511016.img | 8336116 |
| Secure (SSH) runtime image software version 5.1.1 | Standard software image for the Avaya Ethernet Routing Switch 3500 Series | 3500_511017s.img | 8575172 |
| Bootloader software version 1.0.0.3 | Bootloader software for the Avaya Ethernet Routing Switch 3500 Series | ERS3500_b1_0_0_3.bin | 315044 |
| Diagnostic software version 1.0.0.9 | Diagnostic software for the Avaya Ethernet Routing Switch 3500 Series | ERS3500_DIAGS_v1_0_0_9 .bin | 2184461 |
| Software Release 5.1.1 MIB definition files | Management Information Base (MIB) definition files | Ethernet_Routing_Switch_35xx_MIBs_5.1.1.zip | 1378052 |
| EDM Help file zip | A downloadable zip file containing Help information for | ers3500v511_HELP_EDM.zip | 3506152 |

| 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) | ers3500v5.1.1.0.zip | 4259756 |

File names for release 5.1

The following table describes the Avaya Ethernet Routing Switch 3500 Series, Software Release 5.1, software files. File sizes are approximate.

| Module or file type | Description | File name | File size (bytes) |
|---|---|---|-------------------|
| Standard (non-SSH) runtime image software version 5.1.0 | Standard software image for the Avaya Ethernet Routing Switch 3500 Series | 3500_510006.img | 8308820 |
| Secure (SSH) runtime image software version 5.1.0 | Standard software image for the Avaya Ethernet Routing Switch 3500 Series | 3500_510007s.img | 8542212 |
| Bootloader software version 1.0.0.3 | Bootloader software for the Avaya Ethernet Routing Switch 3500 Series | ERS3500_b1_0_0_3.bin | 315044 |
| Diagnostic software version 1.0.0.8 | Diagnostic software for the Avaya Ethernet Routing Switch 3500 Series | 3500_1008_diag.bin | 2184785 |
| Software Release 5.1 MIB definition files | Management Information Base (MIB) definition files | Ethernet_Routing_Switch_35xx_MIBs_5.1.0.zip | 1362955 |
| EDM Help file zip | A downloadable zip file containing Help information for Enterprise Device Manager (EDM) | ers3500v510_HELP_EDM.zip | 3480569 |

| Module or file type | Description | File name | File size (bytes) |
|----------------------|---|---------------------|-------------------|
| COM Plug in file zip | COM Plug in for Enterprise Device Manager (EDM) | ers3500v5.1.0.0.zip | 4245839 |

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_1008_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_3.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 release 5.1 and 5.1.1.

Table 2: 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 | 254 |
| DHCP Server clients per switch/stack | 1000 |
| 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 |
| 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 802.3at (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 5: Resolved issues

Use the information in this section to learn more about issues that have been resolved in Release 5.1 and 5.1.1.

Resolved issues in Release 5.1.1

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

| Reference number | Description |
|-------------------------|--|
| From Release 5.1 | |
| wi01066463 | Autosave: The Backup CONFIG file prevents the corruption of the configuration file in the case of a power failure occurring during the process of writing the configuration to NVRAM, through the creation of an automatic backup configuration file. |
| wi01090862 | EDM: The Local Locations tab can be used to set street, city and state name for E911 on ports. |
| wi01099073 | MIB: The "Mgmt" MIB is compliant with RFC1213. The ipAdEntBcastAddr contains accurate values. |
| wi01101571 | CANA: Speed 10.000 (10 G) cannot be set in this release. |

Resolved issues in Release 5.1

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

| Reference number | Description |
|-------------------------|--|
| From Release 5.0 | |
| wi00986612 | IGMP Snooping: A maximum of 59 IGMP groups is supported by the hardware, not 240 groups as previously reported. |

Resolved issues

| Reference number | Description |
|------------------|--|
| wi00990398 | Port Mirroring: Packets generated by the CPU (such as BPDU, SONMP and LLDP packets) are not mirrored. |
| wi00988662 | ssh: The default SSH parameters cannot be modified from a SSH session using ASCII configuration. |
| wi00990836 | ACG file download from EDM: At this time, users should download the configuration using ACLI only. |

Chapter 6: Known issues and limitations

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 5.1.1

The following table lists and describes known issues and limitations for Avaya Ethernet Routing Switch 3500 Series Software Release 5.1.1. Where available and appropriate, workarounds are provided.

| Reference number | Description |
|------------------|--|
| wi01101821 | EDM/Asset ID: While creating an Asset ID in the CLI, if the "<" character is used, all characters following "<" is truncated in the EDM display. |
| wi01108851 | DHCP Server: The local switch VLAN IP is assigned to a DHCP client if the IP is in IP pool range. The DHCP client identifies the conflict, displays an error message and requests for a new IP. |

Known issues in Release 5.1

The following table lists and describes known issues and limitations for Avaya Ethernet Routing Switch 3500 Series Software Release 5.1. Where available and appropriate, workarounds are provided.

| Reference number | Description |
|------------------|--|
| wi01070932 | 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. |

| Reference number | Description |
|--------------------------|---|
| 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' |
| wi01034083 | MIB walk, EDM: Occasionally the walk performed on 1.3 from EDM may fail due to the EDM timeout. |
| wi01041815 | Image file download: If an image checksum is incorrect, the system returns the following message: % Invalid image |
| wi01048337 | EAP Advance, EDM: 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 |
| wi01056255 | DHCP Server Leases: The IP address of a host type pool is always shown as a leased address in show leases table, no matter if the client actually requested the address or not. |
| 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 |
| wi01059318 | Web/Telnet/Console, EDM: You can only change the authentication type in Web/Telnet/Console tabs in EDM for a single unit. |
| wi01079448 | MIB, Temperature sensor: The Temperature sensor in the 35XX units is currently defined as a "Metro1200ESM" |
| 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 . |
| 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". |
| From Release 5.0 | |
| wi00966215 wi00966455 | 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 |

| Reference number | Description |
|------------------|--|
| wi00968425 | <p>QoS and one by DHCP). In order to enable ADAC/IPSG/UDP Fwd, at least one precedence should be freed.</p> <p>The precedences used by QoS can be freed by issuing the following commands:</p> <pre>(config)# qos if-group name <GROUP_NAME> class <trusted unrestricted> (config)# qos if-assign port all name <GROUP_NAME></pre> <p>The precedence used by DHCP can be freed by issuing the following command:</p> <pre>(config-if)# no ip dhcp-relay</pre> <p>Note that the precedence used by ARP cannot be freed.</p> |
| wi00988287 | <p>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.</p> |
| wi00988195 | <p>sftp syslog: Saving the binary configuration to an external TFTP or SFTP server will generate a <code>bsnConfigurationSavedToNvram</code> message in the Syslog as the configuration is saved in the NVRAM prior sending it.</p> |
| wi00990895 | <p>IPSG: Do not enable IP Source Guard (IPSG) on trunk ports.</p> |
| wi00984443 | <p>Fan Failure: If an ERS 3510GT-PWR+ fan fails, during diagnostics, the Status LED should flash Amber, but the Power LED lights Amber instead.</p> |

