Release Notes — Release 6.3
Avaya Ethernet Routing Switch 5000 Series

6.3
NN47200-400, 07.02
November 2012

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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 Web sites referenced within this site or documentation(s) 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 this product. 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 Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, 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 RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 RESELLER, AND 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”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(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(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 other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Purpose of this document

Purpose of this document

This document describes new features and important information about the latest release. Release notes include a list of known issues (including workarounds where appropriate) and a list of resolved issues. This document also describes known limitations and expected behaviors that may first appear to be issues.

Chapter 2: New in this release

The following sections detail what's new in Avaya Ethernet Routing Switch 5000 Series Release 6.3.

Features

See the following sections for information about feature changes.

802.1AB customization

Release 6.3 supports a wider range of industry standard System TLVs and their respective configuration to provide maximum customer configuration support for IP Phones, FLARE, and other services.

802.1AB, Link Layer Discovery Protocol (LLDP) customization expands LLDP capabilities so that you can customize all of the LLDP advertisements and timers. The enhanced flexibility provided by the additional customization makes LLDP suitable for deployments where a variety of vendor equipment or deployment methods exist.

You can customize the following Type, Length, and Value (TLV) elements for your deployment needs:

- Standard System TLV's
- Port Description TLV
- System Name TLV
- System Description TLV
- System Capabilities TLV
- Management Address TLV
- VLAN Name TLV
- Port VLAN ID TLV
- Port and Protocol VLAN ID TLV
- MAC/PHY configuration/status TLV
- Power via MDI TLV

- Link Aggregation TLV
- Maximum Frame Size TLV
- LLDP MED Capabilities TLV
- Network Policy TLV
- Location Identification TLV
- Extended Power-via-MIDI TLV
- Inventory TLV

You can also configure the following LLDP timers:

- Reinitialization Delay
- Transmit Interval
- Transmit Delay
- Transmit Hold
- Fast Start
- SNMP Notification Interval

802.1AB Integration

With 802.1AB, Link Layer Discovery Protocol (LLDP) integration you can simplify the deployment of Avaya voice solutions with Avaya data products because 802.1AB integration supports a set of Avaya-specific TLVs that you can use to provision and report about parameters that support Avaya IP telephones. When you use the 802.1AB integration TLVs, you achieve a more rapid deployment of voice solutions and you can also view information from the data network about the services the voice solutions use. 802.1AB integration also works with Avaya Energy Saver to maximize off-peak power savings for network and voice services without impact to service.

You can configure the switch to transmit the following optional proprietary Avaya TLVs that are used to provision Avaya IP handsets:

- PoE Conservation Level Request TLV
- Call Server TLV
- File Server TLV
- 802.1Q Framing TLV

802.1AB new default parameters

Beginning with Release 6.3, you can improve Voice and Video over IP function as some of the LLDP parameters are enabled by default. You can connect LLDP enabled IP handsets to the

switch and start deployment without additional configuration. The following per-interface LLDP parameters are enabled by default:

- lldp config-notification
- lldp status txAndRx config-notification
- lldp tx-tlv local-mgmt-addr port-desc sys-desc sysname
- lldp tx-tlv dot3 mdi-power-support
- lldp tx-tlv med extendedPSE inventory location med-capabilities network-policy
- lldp med-network-policies voice dscp 46 priority 6

802.1X non-EAP Accounting

Accounting support is extended to generate accounting messages and interim updates for non-EAP (NEAP) clients. If you configure different servers for EAP and non-EAP clients, the system directs accounting messages to the appropriate EAP and NEAP servers..

802.1X non-EAP re-authentication

You can use non-EAP (NEAP) re-authentication to resolve connectivity issues that occur when devices authenticated by NEAP enter sleep mode or are decommissioned and removed from the RADIUS database and the port the device is connected to is removed from the RAV VLAN. When you use NEAP to authenticate devices such as printers, IP cameras, and card readers, you can set defined re-authentication intervals so that an idle device does not lose network connection and a decommissioned device does not occupy a connection.

When NEAP re-authentication is enabled, the switch sends authentication messages automatically to the RADIUS server at the configured interval, after the first authentication of the NEAP user on the port.

Add DecOtherEther2 to Protocol-Based VLANs

When you disable the filter limiting feature, you can create a larger number of protocol-based filters when an ERS 5510 is not in the stack. A feature enhancement delivers a pre-defined filter for the decOtherEther2 protocol. The protocol PIDs are 0x6000–0x6003, 0x6005–0x6009, 0x8038. Decimal values for these are 24576–24579, 24581–24585, 32824.

The use of decOtherEther2 protocol VLAN is mutually exclusive with a user-defined protocol VLAN from the same PID range.

On a software upgrade, if you are using one of the decOtherEther2 PIDs for private use, the PIDs will still be in place after the upgrade, however the decOtherEther2 protocol VLAN may not be created.

Block Subsequent MAC Authentication in MHMA

Prior to Release 6.3, in MHMA mode, if a station successfully authenticates, the switch places the port in the RADIUS assigned VLAN that corresponds to that station's login credentials. If a second station properly authenticates on that same port, the switch ignores the RADIUS assigned VLAN and the user is placed in the same VLAN as the first successfully authenticated station, creating a potential security risk.

This feature enhancement gives the administrator the option of either using the current implementation or a separate option that will block subsequent MAC authentications if the RADIUS assigned VLAN is different than the first authorized station's VLAN.

Circuitless IP (CLIP)

You can use a circuitless IP (CLIP) interface to ensure connectivity to an ERS 5000 Series device, as long as a network path is available to reach the device. CLIP allows the flexibility of assigning an IP address for various functions without having to physically bind it to an interface.This is useful for routing protocols such as OSPF or BGP where the router ID should be the IP address of an interface that is always up and reachable.

In Release 6.3, CLIP is supported on the default VRF only, with a maximum of 16 CLIPs supported.

Content-Based Forward to Next Hop Enhancements

Enhancements have been made to the Content-Based Forward to Next Hop feature to increase the usability and functionality of this feature:

- per VLAN enable — Release 6.3 enables filter instances to be applied to ports on a per VLAN basis. Policy instances will only be installed on ports that are members of one or more of the VLANs that are attached to the forward to next hop policy.
- Match on TCP/UDP Port — the match criteria is expanded in Release 6.3 to include Layer 4 port numbers/ranges. You can specify a UDP or TCP (or both) port number or port number range in the next hop policy.
- Support Redundant Next Hop for Same Source IP — previous releases limited the next hop to a single destination. You can now configure a secondary next hop should the primary become unavailable or unreachable.

DHCP Snooping External Save

You can use DHCP Snooping External Save to automatically save the DHCP Snooping database once every 5 minutes, to a specified external location, such as a TFTP server or USB drive. The switch can then retrieve stored DHCP Snooping database information from the TFTP server or USB drive on reset, if the SNTP is active and synchronized. This means that for the devices that do not re-request a DHCP lease, the MAC and IP address association found in the DHCP Snooping database is restored, and the renew of the IP address or the reboot of the end device is not required. Furthermore, this feature allows the switch to maintain current DHCP assignments for active devices which do not re-request IP assignments in response to a link down/up event, as caused by a switch reset.

Diagnostic Auto Unit Replacement

Diagnostic Auto Unit Replacement (DAUR) enables the switch to update the diagnostic image of the non-base unit with the diagnostic image saved in the base unit of a stack, in the same way that Agent AUR (AAUR) performs this function for agent code. You must enable AAUR on the stack first. When you enable or disable AAUR, you also enable or disable DAUR. The default for AAUR is enabled. There are no commands to separately enable or disable DAUR.

The diagnostic combo image AUR is also introduced with this release. The diagnostic combo image consists of two images, a 56xx image and a 55xx image, concatenated together. A combo image is required since the 56xx diagnostic is not compatible with the 55xx diagnostic. Note that the expected behavior of the combo diagnostic AUR is similar to the combo agent AUR.

Disable CLI Audit

The enhancement to the CLI Audit feature allows you to disable the feature in which all CLI commands are logged automatically. The CLI Audit feature is enabled by default.

IGMP Multicast Flood Control

IGMP multicast flood control limits IP multicast traffic without inhibiting other control protocols. By minimizing IP multicast flooding in the network, it eliminates the necessity of queries sent by the switch when IGMP snooping is enabled.

IGMP multicast flood control is available on the ERS 5520/5530/5600 products in Release 6.3 (ERS 5510 is not capable of supporting this feature).

IGMP over SMLT

Release 6.3 introduces the ability to support Internet Group Management Protocol (IGMP) over Split Multilink Trunking (SMLT) network topologies..

Increased ARP Table Size

The maximum limit of dynamic ARP table entries supported increases from 1,500 to 2,500 on the ERS 5600 products to enable support for larger networks. If the new limit of 2,500 entries is reached, additional entries are rejected. New entries can be learned and populated in the table as entries age out, until the maximum has been reached. The new limit is supported for ERS 5600 products operating in a pure mode (stacked or standalone). When an ERS 5500 product is placed within the stack, the previous limit of 1,500 entries will be the maximum table size.

Increase MAC Filtering List support

Release 6.3 increases the maximum number of entries in the MAC Filtering List from 32 to 128.

Inexistent VLAN Mapping for MSTI

Inexistent VLAN mapping for MSTI makes it easier for Avaya products to interoperate in heterogeneous environments by mapping VLAN ranges to MSTI intances for the purpose of MSTP Region Config Digest calculation without requiring you to actually create VLANs.

Internal BGP

The Ethernet Routing Switch 5600 can use internal Border Gateway Protocol (iBGP) to communicate within a single Autonomous System (AS). ERS 5600 does not support external BGP (eBGP) for communication between multiple external ASs, or full-table BGP Internet downloads.

The following BGP functions are supported in Release 6.3:

- iBGP (eBGP will be supported in a future software release)
- BGP Route Reflector
- BGP Aggregation

- BGP Redistribution
- Circuitless IP (CLIP)
- BGP ECMP

IP Manager support for SSH

IP Manager can limit access to the management features of the Avaya ERS 5000 Series by defining the IP addresses that are allowed to access the switch. SSH enhancements have been added to allow you to:

- define up to 50 IPv4 addresses and masks and up to 50 IPv6 addresses that are allowed to access the switch from SSH
- enable or disable access to SSH

Lossless Mode Support for 8–High Stack

Release 6.3 removes the restriction of 5 units maximum in a stack to allow support for 8 units within a stack operating with lossless mode configured.

MLT/DMLT/LAG Dynamic VLAN Changes

Enhancements have been made to the operation of Link Aggregation Groups (LAG) so as to provide consistent operation of Multi-Link Trunk (MLT), Distributed Multi-Link Trunk (DMLT), and LAGs. Now you can make dynamic VLAN changes (that is addition or removal) on any trunks without disabling the trunk first. This is an important improvement in that it allows you to make VLAN changes on any trunks while keeping them in service.

PIM-SSM

The Ethernet Routing Switch 5000 Series supports the source filtering capability for IGMPv3 using PIM-SSM (IGMPv3 routing mode). IGMPv3 routing mode works only with PIM-SSM and is not backward compatible with IGMPv1 or IGMPv2 .Source Specific Multicast (SSM) optimizes PIM-SM by simplifying the many-to-many model . SSM uses a one-to-many model that only uses a subset of the PIM-SM features . This model is more efficient and puts less of a load on multicast routing devices.

RADIUS EAP/non-EAP different servers

You can now separate EAP and non-EAP (NEAP) functions by server. You can configure up to two RADIUS servers, either IPv4 or IPv6, for authentication and accounting of EAP requests,

and up to two servers, either IPv4 or IPv6, for authentication and accounting of NEAP requests.

If you do not explicitly configure servers for either EAP or non-EAP requests, the switch uses the normal RADIUS server(s) configuration.

Note:

Because SHSA and MHSA modes do not support the authentication of non-EAP clients, ports in SHSA or MHSA mode do not use non-EAP RADIUS servers for authentication.

RADIUS Management Accounting with TACACS+ support

RADIUS Management Accounting provides the ability to send RADIUS accounting packets for management events such as user login/logout, session time-outs for a logged in user, etc. When enabled, this feature allows TACACS+ related messages to be transmitted to the RADIUS server.

RADIUS Support for Interim Accounting

RADIUS Accounting Enhancement (RFC2866) provides the ability for the switch to send detailed RADIUS accounting updates to the RADIUS server based on the configured update interval.

Instead of providing summarized information only after RADIUS Accounting was stopped, new support for Interim Accounting has been added so that you can specify intervals for interim accounting information while accounting is enabled. Information contained within the interim messages are the same as those included in the accounting stop message, with the exception of the termination information. The accounting information is cumulative from the accounting start phase versus being incremental between interim messages.

The implementation of this functionality and in particular the Framed-IP-Address attribute provides significant improvements for the integration with the Identity Engines security platform.

Routing of IP Directed Broadcasts on a per VLAN basis

In previous releases, routing of IP directed broadcasts was enabled globally on a switch or stack. In Release 6.3, you can enable or disable this functionality on a per VLAN basis.

When upgrading the switch to Release 6.3, this feature is enabled globally as well as on all L3 VLANs in order to maintain seamless functionality.

Serial Security Enhancement

With the Serial Security feature the switch logs you out if the serial console is removed from the port. You are prevented from opening a new session without closing the current one. A second device cannot connect illegally as the logout action secures the console interface against the potential security risk.

Show Software Status

This feature enables you to determine the status of the software downloaded to the switch. You can download a new image to the switch and choose the no-reset option. This allows you to download the new software, but the software will not take effect until you reset the switch.

The information is shown in the following commands:

- show boot
- show sys-info
- show tech
- show license

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 appropriate log messages and SNMP traps.

SNMP Trap Enhancements

SNMP trap enhancements allow you to enable or disable notifications for objects on specific interfaces, as well as globally. All notifications are enabled by default, globally and per interface, while certain SNMP traps are supported per interface, except OSPF-TRAP-MIB traps which are disabled by default. You can modify these notifications according to your requirements using SNMP trap notification control.

SSH Banner

Prior to Release 6.3 the SSH banner was displayed to a user after a successful login. With the need for increased security requirements, you can configure a customized SSH banner for the SSH clients. This banner displays before completing the SSH login, prior to entering the password. This ensures the awareness of the institution's security policy. The default setting is for no banner.

SSH retry

Prior to Release 6.3, if you enter incorrect SSH login credentials, the session terminates. To add more flexibility to this security mechanism, the administrator can configure the number of retries the user is allowed before the connection is terminated.

Static MRoute for PIM

This feature allows some separation of multicast and unicast traffic in routed networks by providing a static router for the multicast traffic. These static multicast routes are programmed into a separate table used only by PIM-SM and PIM-SSM and are not visible to any other unicast traffic. In the absence of a defined static multicast route, traditional unicast routes are selected.

Sys-uptime Pre-notification Trap

When a switch unit has been continuously operating for 365 days, this feature produces a SNMP trap to notify the administrator. This trap allows ample time to plan for a reset during a scheduled maintenance window, or to schedule one if none exists. Once the switch has been reset, the counter starts over at 0 and will send out another trap when 365 days of continuous uptime has been reached. For a stack, a physical stack event should not affect this feature, since the trap is sent when the counter for the base unit is 365 days.

Syslog Support for 802.1X/EAP/NEAP/UBP

Syslog messages for the various states of 802.1X/EAP/NEAP/UBP authentications are introduced to allow more thorough troubleshooting. Logged messages include: time of authentication, MAC authentication success/fail, IP address associated with MAC authentication, and VLAN and UBP policy assignment.

Trace Support for 802.1X

A Trace command previously available for various applications (OSPF, RIP, SMLT, IPMC, IGMP, and PIM) now also supports 802.1X/EAP, in 4 levels for each module or application. All previous levels of Trace are supported, i.e. Very Terse, Terse, Verbose, and Very Verbose. The higher the level requested, the more information is displayed.

Unified User Authentication

With Unified Authentication, you can manage only one set of local username and password 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. If you downgrade the switch to a previous software release the switch updates the obsolete standalone authentication method, username, and local passwords to ensure maximum compatibility.

Unified User Authentication options can also be changed using EDM.

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.

VRF Lite

This release supports Virtual Routing and Forwarding (VRF) Lite for the ERS 5600 platform only. VRF Lite gives you the ability to deploy multiple virtual routing instances over the same physical hardware, essentially turning a single switch into multiple routers. With VRF Lite, you can reduce operating costs by employing virtual router instances to maintain networking capabilities and traffic isolation for clients operating over the same physical router.

This initial release of VRF Lite consists of four VRF instances (VRF0, VRF1, VRF2, and VRF3). VRF0 is referred to as the default VRF or global instance. Dynamic routing is supported only

on VRF0 while static routing can be utilized on VRF1–3. All VRF instances support DHCP Relay.

Other changes

Release 6.3 introduces the new guide, *Avaya Ethernet Routing Switch 5000 Series Getting Started* (NN47200–303). The information contained in the Getting Start guide is a subset of the *Avaya Ethernet Routing Switch 5000 Series Configuration-System* (NN47200–500). Other information previously contained in the *Avaya Ethernet Routing Switch 5000 Series Configuration System* (NN47200–500) document has been moved appropriately to other configuration books in the ERS 5000 documentation suite.

For a summary of the current documentation suite for the ERS 5000, refer to the *Avaya Ethernet Routing Switch 5000 Series Documentation Roadmap* (NN47200–103).

Chapter 3: Introduction

This document describes new features, hardware, upgrade alerts, known and resolved issues, and limitations for the Avaya Ethernet Routing Switch 5000 Series, Release 6.3

The Avaya Ethernet Routing Switch 5000 Series includes the following switch models:

- Avaya Ethernet Routing Switch 5510-24T
- Avaya Ethernet Routing Switch 5510-48T
- Avaya Ethernet Routing Switch 5520-24T-PWR
- Avaya Ethernet Routing Switch 5520-48T-PWR
- Avaya Ethernet Routing Switch 5530-24TFD
- Avaya Ethernet Routing Switch 5698-TFD
- Avaya Ethernet Routing Switch 5698-TFD-PWR
- Avaya Ethernet Routing Switch 5650-TD
- Avaya Ethernet Routing Switch 5650-TD-PWR
- Avaya Ethernet Routing Switch 5632-FD

Configurations can vary from a standalone switch to a stack of up to 8 switches. A stack can consist of any combination of switches. One benefit of operating Avaya Ethernet Routing Switch 5000 Series switches in a stack is management efficiency; a stack is managed with a single IP address and software is available as a single image across all models.

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

For a complete list of documentation in the Avaya Ethernet Routing Switch 5000 Series suite, see *Avaya Ethernet Routing Switch 5000 Series Documentation Roadmap, NN47200-103*.

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

Chapter 4: Important notices and new features

This section describes important software and hardware related notices in the Avaya Ethernet Routing Switch 5000 Series Release 6.3.

Feature document location

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

Table 1: Where to find information about key software features

Feature	Document
QoS Traffic Profiling Support	*Avaya Ethernet Routing Switch 5000 Series Configuration - Quality of Service* (NN47200-504)
SMLT configuration	*Avaya Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and Link Aggregation* (NN47200-502)

Release file names

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

Table 2: Release 6.3 software components

File Type	Description	File Name	File Size (bytes)
Standard runtime combo image software version 6.3	Standard non SSH combo image for the Ethernet Routing Switch 5000 Series	5xxx_630012.img	19,271,500
Secure runtime combo image software version 6.3	Standard SSH combo image for the Ethernet Routing Switch 5000 Series	5xxx_630013s.img	20,068,628

File Type	Description	File Name	File Size (bytes)
Combo diagnostic software version 6.0.0.15	ERS 5000 Combo diagnostic software	5xxx_60015_diags.bin	2,467,848
Enterprise Device Manager Help Files	EDM Help files zip	ERS5000v630_HELP_EDM.zip	2,140,362
MIB Definition File	MIB Definition File	Ethernet_Routing_Switch_5xxx_MIBs_6.3.0.zip	1,769,131
COM Plug in	ERS 5000 plugin for COM	ers5000v6.3.0.war	3,660,190

Software upgrade

The procedures in this section are used to upgrade the diagnostic and agent software. Use these procedures to upgrade to Software Release 6.3.

Important:

There is no upgrade path from any agent software release earlier than 6.2 to Software Release 6.3. Devices running older agent software must first be upgraded to a version of Software Release 6.2 before upgrading to Software Release 6.3. Note that the diagnostic software running on the device should not be earlier than 6.0.0.15.

Important:

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

Upgrading diagnostic software

Use the following procedure for upgrading the diagnostic software image.

1. Access the ACLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the **enable** command.
3. Use the command **download address <ip_address> diag <image_name> [no-reset] [usb]** to transfer the diagnostic image to the device.

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

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the diagnostic image is hosted.
diag <image_name>	The name of the diagnostic image file on the TFTP server.
no-reset	This parameter specifies that the device will not reset after the upgrade is complete.
usb	This parameter specifies that the software download will occur from a USB device instead of the network. This option is only valid with the 5530-24TFD and 5600 Series devices.

The upgrade process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process.

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

During the download process the switch is not operational.

Upgrading agent software

Use this procedure to upgrade agent software.

1. Access the ACLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the **enable** command.
3. Use the command **download address <ip_address> {primary | secondary} {image <image_name> | image-if-newer <image_name> | poe_module_image <image_name>} [no-reset] [usb]** to transfer the agent image to the device.

The following table describes the parameters for this command.

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the agent image is hosted.
primary | secondary	Designates whether the image is stored in the primary or secondary image location. The default is primary.
image <image_name> | image-if-newer <image_name> |	The name of the agent image file on the TFTP server. Each option is mutually exclusive. Use the option described with the following situation:

Parameter	Description
poe_module_image <image_name>	• To load the agent image under normal circumstances, use the image option. • To load the agent image only if it is newer than the current image, use the image-if-newer option. • To load the agent image if it is a PoE module image, use the poe_module_image option.
no-reset	Specifies that the device will not reset after the upgrade is complete.
usb	Specifies that the software download will occur from a USB device instead of the network. This option is only valid with the 5530-24TFD and 5600 Series devices.

The upgrade process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process.

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

During the download process the switch is not operational.

How to get EDM online help files for embedded EDM

Because help files are not included with the embedded EDM software files on the switch, a network administrator must copy the software-release-specific help files onto a TFTP server. Once the help files are downloaded to the TFTP server, the network administrator must configure the switch with the path to the help files on the TFTP server. You can use ACLI or EDM to configure a path from your switch to the help files. After the path to the help files is configured, whenever an EDM user clicks the help button on the toolbar, the switch downloads and displays help information in the Web browser.

If you are using Configuration and Orchestration Manager (COM) to manage your switch, help resides with COM and you do not need to use these procedures.

For more information about EDM, see *Avaya Ethernet Routing Switch 5000 Series Fundamentals, NN47215-102*.

Downloading help files

Before you begin

- An available TFTP server

About this task

Use this procedure to download EDM online help files.

Procedure

1. To obtain EDM help files for the embedded element manager, do one of the following:
   - Go to the Avaya Web site at http://www.avaya.com/support and locate the help files for the appropriate product.
   - Select the help files from the software CD ROM.
2. Download the help files to a TFTP server.

How to configure the path to the embedded EDM help files

If you are using embedded EDM, use the procedures in this section to configure the path to the help files. You can configure the help file path with ACLI or EDM.

Configuring the path to the help files using ACLI

About this task

Use the following procedure to configure the path to the help files using ACLI.

Procedure

In ACLI, go to the Global Configuration mode and use the following command:

```
edm-help-file-path <path name> tftp address <tftp address>
```

The following table describes the parameters for the edm-help-file-path command.

Parameter	Description
path name	Specifies the path name you created for EDM help files. The path name is stored in NVRAM.

Parameter	Description
TFTP address	Specifies EDM TFTP server IP address. Use this address only for EDM help files. If you do not specify a TFTP server address, the system uses the address specified most recently. WARNING: Because the TFTP server address is stored in NVRAM, each time the system returns to the default configuration, you must reconfigure the path to EDM online help.

Example

Following is an example of an ACLI EDM help file path:

```
edm help-file-path ERS5000_63_Help tftp address 100.100.100.15
```

In the preceding example ERS5000_63_Help is a folder that contains help files and the folder is located on a TFTP server at the 100.100.100.15 address.

Configuring the path to the help files using EDM

Use the following procedure to configure the path to the help files.

Procedure steps

1. From the navigation tree, click **Edit**.
2. From the Edit tree, click **File System**.
3. Select the **Help File Path** tab.
4. In the Path dialog box, enter the path to the help file storage location.

   Example

   tftp://xxx.xx.x.x/file_name

Supported software and hardware capabilities

The following table lists the known limits for the Avaya Ethernet Routing Switch 5000 Series, Release 6.3 and Enterprise Device Manager.

Table 3: Supported software and hardware capabilities

Feature	Maximum number supported
VLANs	1024 (1k)
Protocol-based VLANs	Depending on the protocol specified, the number of protocol VLANs supported at one time varies between 3–7. See *Avaya Ethernet Routing Switch 5500 Series Configuration — VLANs, Spanning Tree, and MultiLink Trunking, NN47200-502* for more information.
NSNA VLANs	One Red VLAN per switch. Avaya recommends a maximum of five Yellow VLANs, five Green VLANs, and five VoIP VLANs per switch.
NSNA ports	All ports. **Note:** The ERS 5530 has two 10 Gigabit (Gb) ports that you can configure as uplink ports only, but not as dynamic ports.
IGMP maximum number of unique groups	Layer 2 and Layer 3 240 IGMP Op-Mode = 5510 492 IGMP Op-Mode = Non-5510 (Hybrid) 992 IGMP Op-Mode = Non-5510 (Pure)
EAPoL 802.1x supplicants	32 per port 768 per stack
Maximum number of routes (dynamic, static and local)	4000 routes for ERS 5600 units and pure stacks (5600 units only) 2000 for hybrid stacks (5500 and 5600 units) and ERS5520/5530 units 512 for ERS 5510 units
ARP records	1500 for ERS 55xx and hybrid stacks 2500 for pure ERS 5600
Static ARP	256
IP interfaces	256
Static routes	512
Spanning Tree Groups	8
IPv6 DHCP relay forward paths	256
IPv6 static routes	512
IPv6 interfaces	256

Feature	Maximum number supported
IPv6 tunnels	4
Aggregation groups (link aggregation)	32
Ports per aggregation group	8
MAC addresses in fdb	16 Kb
OSPF areas	4 (3 areas plus area 0)
OSPF adjacencies	64
VRRP interfaces	64
ECMP	4 paths (not supported on ERS 5510 switches.)
DHCP Snooping Binding table entries	1024
DHCP relay forward paths	512
IP Management routes	4
PIM-SM multicast entries	Up to 492 for ERS 55xx series Up to 992 for ERS 56xx series The hardware for ERS 55xx platforms supports a maximum of 492 IPMC forwarding entries. The ERS 56xx platforms support a maximum of 992 IPMC forwarding entries. These limitations are imposed on standalone ERS 5xxx devices and stacks with the added limitation that, on hybrid stacks, the lower limit of 492 IPMC forwarding entries is imposed. Note: These limits do not indicate that 492 or 992 entries will actually be available since the installation of IPMC entries in hardware is also determined by free entries being available. Also, on ERS 5510 platforms, the available number of IPMC forwarding entries is 240. Note: ERS 5510 units cannot participate in PIM-SM due to hardware limitations.
Allow-flood IGMP multicast addresses	The maximum number of allow-flood multicast entries is determined by the number of VLANs on the device. Each entry in the allow-flood table applies to each current VLAN; for example, if 1 entry exists in the allow-flood table and 5 VLANs are configured, then there are 5 entries programmed in hardware. Currently, the

Feature	Maximum number supported
	hardware limit is 4096. Note: You should not exceed this limit. The limit for the maximum number of allow-flood addresses is 128 (1 VLAN).

Avaya Ethernet Routing Switch 5520 phone dongle

The part number for the Avaya Ethernet Routing Switch 5520 (5520-24T/48T-PWR) universal phone dongle is DY4311046.

Additional information for the software feature license file

When you create a license file to enable licensed features on an Avaya Ethernet Routing Switch 5000 Series switch with the Avaya Electronic Licensing Portal, you must specify a file name. Follow the instructions on the License Certificate within the License Kit, or for more information, see *Avaya Ethernet Routing Switch 5000 Series Fundamentals, NN47200-104*.

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

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

File name example, abcdefghijk_1234567890.lic.

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

- ASCII file format
- One MAC address per line
- No other characters, spaces, or special characters allowed
- MAC must be in hexadecimal, capitalized format, with each pair of characters separated by colon; for example, XX:XX:XX:XX:XX:XX

- The file must contain the correct MAC addresses. Any incorrect MAC addresses will result in the licensed features not working on designated units.
- The number of MAC addresses must not exceed the number of MAC addresses allowed for the License Authorization Code entered for a particular file. For example:
  - AL1016001 = 2 MAC addresses (1 stack/standalone unit)
  - AL1016002 = 20 MAC addresses (10 stacks/standalone units)
  - AL1016003 = 100 MAC addresses (50 stacks/standalone units)
  - AL1016004 = 200 MAC addresses (100 stacks/standalone units)

Supported standards, MIBs, and RFCs

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

Standards

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

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1X (EAPOL)
- IEEE 802.1ab (Link Layer Discovery Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow Control)
- IEEE 802.3z (Gigabit Ethernet)
- IEEE 802.3ab (Gigabit Ethernet over Copper)
- IEEE 802.3ad (Link Aggregation)

RFCs

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

- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 894 (IP over Ethernet)
- RFC 951 (BootP)
- RFC 1112 (IGMPv1)
- RFC 1157 (SNMP)
- RFC 1213 (MIB-II)
- RFC 1271 (RMON)
- RFC 1350 (TFTP)
- RFC 1493 (Bridge MIB)
- RFC 1757 (RMON)
- RFC 1945 (HTTP v1.0)
- RFC 2131 (DHCP)
- RFC 2236 (IGMPv2)
- RFC 2362 (PIM-SM)
- RFC 2474 (QoS)
- RFC 2597 (QoS)
- RFC 2598 (QoS)
- RFC 2665 (Ethernet MIB)
- RFC 2674 (Q-BRIDGE-MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2865 (RADIUS)

- RFC 3140 (QoS)
- RFC 3246 (QoS)
- RFC 3410 (SNMPv3)
- RFC 3411 (SNMP Frameworks)
- RFC 3412 (SNMP Message Processing)
- RFC 3413 (SNMPv3 Applications)
- RFC 3414 (SNMPv3 USM)
- RFC 3415 (SNMPv3 VACM)
- RFC 3576 (Dynamic Authorization Extensions to Remote Authentication Dial In User Service)

The following table lists IPv6 specific RFCs.

Standard	Description	Compliance
RFC 1886	DNS Extensions to support IPv6	Supported
RFC 1981	Path MTU Discovery for IPv6	Supported
RFC 2460	Internet Protocol v6 (IPv6) Specification	Supported
RFC 2461	Neighbor Discovery for IPv6	Supported
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 3162	RADIUS and IPv6	Supported
RFC 3315	DHCPv6	Support for IPv6 DHCP Relay
RFC 4007	Scoped Address Architecture	Supported
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Not supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack and configured tunnels

Standard	Description	Compliance
RFC 4291	IPv6 Addressing Architecture	Support earlier version of RFC (3513)
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4301	Security Architecture for the Internet Protocol	Not supported
RFC 4443	Internet Control Message Protocol (ICMPv6)	Support earlier version of RFC (2463)

Chapter 5: Resolved issues

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

Change Request Number	Description
wi00491923	The system does not remove all expired MAC Source Addresses in the MAC Address Table after the aging time has expired.
wi00484828, wi00492144, wi00497730	Device Type for devices connected to the data port on a VoIP phone are being displayed as UNKNOWN instead of PASSIVE in the command output of show nsna client.
wi00492820	ADAC port configuration types not defined in manual.
wi00485407	Unnecessary system messages of STP_CLR_PCONFIG: PCFG_BRIDGING stpgId 0, portNo x are generated when disabling spanning tree on Ethernet ports.
wi00493682, wi00495091, wi00497859	Informational event type information is being sent to remote syslog server even when Event Type To Log is restricted to Critical and Serious event types.
wi00493706	No confirmation message is provided when an ASCII configuration, initiated via the UI (User Interface) push button, is successfully uploaded to the USB port.
wi00486074	Time Domain Reflector test ran from JDM is returning Pair Shorted as an error message for Pin Short cable problems rather than the correct error message of Pin Short.
wi00493776	MAC security Lifetime setting cannot be modified from the JDM.
wi00486100	MAC authorized clients are not reauthorized after a former base unit rejoins the stack.
wi00486318	LLDP configuration within an ASCII configuration file may fail to load during an ASCII configuration upload.
wi00486328	The cost metric, within the show ip routes output, for external routes increases to 127174722 when a fictitious OSPF virtual link is created than deleted.
wi00486432, wi00486962, wi00496973	The system does not remove user based policies nor age out the MAC addresses of Non EAPOL clients that physically migrate to a different EAPOL enabled port. This behavior will result in Non EAPOL authentication failure for migrating clients when attempting to authenticate and applying policies on their new ports. Error state will generate the following system messages: Duplicate users (different port, same user name) and bsnEapUbpFailure prohibited.

Change Request Number	Description
wi00486497	Unknown multicast and known multicast variables within a system classifier are not functioning correctly. Issue is exclusively on the 5600.
wi00486386	Multicast traffic is not forwarded to the destination network configured within a non-local static route (NLSR). A NLSR is similar a regular static route except that the next hop of a NLSR static route is not directly connected
wi00486635	The source IP address for traffic destined for a RADIUS server should be the IP address of the Management VLAN IP interface.
wi00494290	PIM is intermittently being disabled on random VLAN interfaces after a reboot.
wi00494367	Incorrect error message of "Invalid file name" is being generated when attempting a software download from an unreachable server.
wi00486652, wi00488134, wi00489324, wi00496995	Uploading an ASCII configuration containing IP route commands results in configuration upload failure and the following system messages: % Cannot modify settings % Duplicate Route Entry. Use Modify Operation
wi00494385	IPv4 and IPv6 IP Addresses stored within NVRAM are not overwritten by the IPv4 and IPv6 Addresses existing in the ASCII configuration file being uploaded to the unit/stack.
wi00486691	Some ARP, OSPF, or VRRP packets are unexpectedly mirrored when using XrxYtx mirroring mode and the monitored port is in the Management VLAN or in SMLT VLANs.
wi00486687	MAC addresses are lost when a base unit fails.
wi00486701	LLDP-Med fails to configure VoIP phones with defaulted configuration. VoIP fails to initiate displaying error messages of "Starting DHCP..." or "DHCP server unreachable..".
wi00486698	ADAC syslog messages sent by non base units is displaying ADAC: System operationally during a system reboot. During a system reboot ADAC is down. The base unit sends the correct syslog message of ADAC: System operationally dis abled
wi00486715	On a pure 56xx stack, port mirroring mode XrxYtx multiplies unicast traffic on port Y in certain scenarios.
wi00486712	Disabling and re-enabling VLACP followed by a reboot will result in VLACP failing to function after the system restores from a reboot.
wi00486688	The EAP-TLS or PEAP-MsChapV2 clients could be unexpectedly transitioned to the EAP Held state on a multihost enabled port.
wi00486710	Voice traffic is blocked on a non-base unit when ARP inspection is enabled on a VoIP VLAN.
wi00494406	Walking the ipNetToPhysicalPhysAddress MIB results in a system reboot with various data access exception tasks of tLDT, tSNMP or bcmRX.

Change Request Number	Description
wi00494771	The LLDP Med-Network-Policies Voice Tagging command is rejected and deemed invalid by the operating system when attempting to execute the command.
wi00494479	PIM outgoing interfaces may not be installed in the r × r identity matrix (IR) if session directory tool (SDR) is flapped.
wi00494624	Continuous IPv6 ping stops working after 2147 ICMPv6 messages.
wi00486941	Telnet session hangs on ERS 5510-48T during an ASCII configuration download.
wi00487092	ACG fails to function if a ports tagging mode is Untagpvidonly and the port is also member of 2 Spanning Tree Groups.
wi00494933	After booting to default setttings the syslog will display the message **ASCII failed at line 1**. This can be ignored. This only happens after a boot to default settings and not during a normal operation or reset of the switch. This does not affect subsequent ASCII downloads. The successful application of configurations can be confirmed using the **show logging** command. The bogus message will be the first in chronological order.
wi00992380	The correct argument order when uploading the sshc key to an usb device and specifying a certain unit is :**sshc upload-host-key usb unit 1 key-name word dsa**.

Chapter 6: Known issues and limitations

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

Known issues

See the following table for a list of known anomalies for the Avaya Ethernet Routing Switch 5000 Series release 6.3.

Table 4: Known issues

Change Request number	Description
wi00906543	EDM, 10G Ports: 10G ports are not seen in EDM under Power Management > PoE > PoE Ports.
wi00927200	NEAP, MHSA Configuration: When a disconnect message is sent for an authenticated EAP user in MHSA mode, you may experience a 15 second delay before the port reverts to the initial VLAN (or Guest VLAN).
wi00929935	Change in ADAC tagged frames configuration: You must delete LLDP MED network policies on phone and uplink/call server ports before configuring ADAC. There are default LLDP MED network policies on all ports that take precedence over ADAC policies.
wi00932580	NEAP, EAP clients and bsnEapRAVError trap: The bsnEapRAVError trap is generated only for EAP clients and not for NEAP clients.
wi00933750	RIP out policy: RIP out policy using network prefix to drop specific networks will not forward other route networks learned from OSPF, static, and direct routes. **Workaround**: Make a sequence 2 in the same route policy to forward any protocol.
wi00941086	Hybrid stack configuration: After booting a default hybrid stack, all 55xx units may experience a delay of 7 minutes or more to achieve link-up. **Recommendation**: Use the boot partial-default command to default a hybrid stack.
wi00960304	EDM, ip-fwd-nh policy: When you create an ip-fwd-nh instance from the base unit using EDM, the policy may fail to attach to a port based VLAN.

Change Request number	Description
wi00982958, wi01001510	MSTP, MLT: When you attempt to enable STP learning on a MLT for an inactive MSTI, you may encounter an error message stating that the corresponding STP is not active, rather than stating that the MSTI is not active.
wi00982961	TACACS+, access mode log message: After connecting to the switch via Telnet/console with TACACS+ enabled, the access mode log message indicates `no security`.
wi00983765	SSH Banner has only ACLI support (no EDM support).
wi00987283	USB devices: USB devices with NTFS or exFAT file format are not supported. FAT32 is the only supported file format.
wi00992287	MAC Security, MAC address table: If you have a MAC security list that has only ports from a unit which is no longer part of the stack, the MAC addresses that are statically associated with the MAC security list are not removed from the MAC address table, even though the MAC security list has been erased. **Workaround**: Manually remove the static entries.
wi00993260	Multicast Group Scaling: When changing the IGMP op-mode to non-5510 on a hybrid stack with 5510 units and the number of learned groups crosses the one supported on the 5510 platform (240), some errors will appear in the consoles of the 55xx units due to hardware limitations.
wi00994307	EDM, IGMP: The 'in port' for IGMP groups is not displayed correctly in EDM. **Workaround**: Display in ACLI.
wi00995161	RADIUS Management Accounting: When accounting is enabled/ disabled from a Telnet/SSH session, NAS-Port-Type contained in the accounting packet is set incorrectly to Async, instead of Ethernet.
wi00996182	TBU, MLT: In a stack configuration, MLT trunk members for units that are temporarily not part of the stack (for example in a reboot process) are still attached logically in the configuration of active units. This event will not show aggregated ports as they will be dynamically hidden in CLI and ACG while the missing unit is not available.
wi00997543	Port Driver Statistics: 55xx: Due to a hardware limitation, only 55xx based ports support Asymmetric Flow Control.
wi00999173	Multicst traffic, IGMPv3: Multicast traffic is not received on the expected port after sending IGMPv3 host reports on 5510 units.
wi01000569	SNMPv3 user: When you create a new SNMPv3 user with password security disabled, using a password string within the required length but with an atom that repeats twice (for example, the password string '12341234'), the user will not be created.

Change Request number	Description
wi01001707, wi01001716	IGMP/SMLT: On stackable switches where Spanning Tree is enabled on VLANs/ports, the following behavior can be expected due to the Spanning Tree convergence time. 1. There will be a 30 second delay of multicast traffic before traffic can be forwarded to MC clients connected on the base unit of the stack when a non-base unit is rebooted. 2. When the non-base unit rejoins the stack, there will be a delay of approximately 90 seconds before the multicast traffic can be forwarded to the multicast clients connected to the non-base unit. MC clients connected to the base unit experience the same behavior as in #1.
wi01007577	DHCP Snooping filename: The maximum length of the DHCP Snooping external filename varies between ACLI and EDM.
wi01007809	RADIUS accounting: When you log off a telnet/ssh session, the RADIUS accounting STOP session message sent indicates an incorrect Acct-Terminate-Cause of `Lost-Carrier` instead of `User-Request`.
wi01009057	Security log messages: When you log out from an SSH session, you may see security log messages of `lost connection` instead of `user logout`.
wi01009215	AUR Auto-Save: The Auto Unit Replacement Auto-Save parameter value is not saved when autosave is set to disabled.
wi01009777	IPFIX — EDM-Offbox: You may be unsuccessful in applying settings for a large number of ports from EDM-Offbox on a SNMPv3 discovered device. Reducing the number of selected ports will yield the expected result.
wi00993819	ADAC — ACLI-EDM inconsistency for UFB and UFA: If ADAC is configured as untagged frames basic or advanced, in EDM tagging appears to be enabled for phone ports, although tagging is disabled for phone ports from the view in ACLI. In ADAC untagged frames basic and advanced, LLDP policies on phone ports are untagged
wi01038367	SSL Certificate/RSA key generation: When the switch generates an SSL certificate at the same time the RSA host key is generated, the CPU may be busy for a short time, as the two activities can be resource intensive.
wi00935460	LACP : When booting a system with one or several LAGs configured, the trunk IDs of the LAGs might not be the same after the system comes up again. The only way to predict this is on an SMLT-LACP environment where the LAG ID is bound to an LACP key
wi00983785	Security, Dynamic ARP: When Dynamic ARP Inspection is configured and ARP packets with invalid IP/MAC bindings are received on

Change Request number	Description
	untrusted ports, traps may be generated for the first port on the corresponding unit on which the invalid ARP packet is received.
wi01010916	QoS: Disabled but not deleted QoS policy data can impact resource utilization. Avaya recommends that you delete QoS policy data that is not required for long term configuration, as opposed to simply disabling the QoS policies. If you experience unexpected resource allocation issues and disabled QoS policies are present, the initial step towards alleviating the resource issue is to delete the currently disabled QoS policies
wi01020873	IGMPv3: IGMPv3 traffic is doubled when port mirroring is configured to mirror the mrouter port on the L2 device (with IGMPv3 snooping enabled) on which the IGMP receiver is connected. You may experience this issue with port mirroring modes: Xrx, XrxOrXtx, manytoOneRx, manytoOneRxTx.
wi01028901	L2, SMLT: On stacks that are involved in IST configuration with the IST links being VLACP enabled with a short time-out value, VLACP brings down the IST during the stack formation process due to lack of VLACPPDUs received. After the rebooted stack is formed again, the IST recovers as soon as VLACPPDUS are received. Workaround: Set a timeout-scale timer value larger than 6.
wi01030591	EDM, QoS statistics : When using QoS statistics for Traffic Profile from EDM, EvalOrder will not be correctly shown on ports from non-base units if the same Traffic Profile set uses multiple eval orders (non block configuration). QoS statistics work as expected on ports from the base unit.
wi01030811	Filter Limiting: Settings made while filter limiting is disabled (more protocol filter entries) are not seen when filter limiting is enabled (fewer protocol filter entries), but the entries are retained. When filter limiting is subsequently disabled and the switch/stack is rebooted, these retained entries will be activated unless changes made while filter limiting was enabled have created conflicts with the retained entries. You do not typically need to switch between settings. If you do, and at the same time you are changing the protocol VLANs, you need to exercise caution or the results when filter limiting is disabled may not be as expected. Changes made while filter limiting is enabled will override those that are retained in the expanded protocol filter list.
wi00946819	Port name is limited to 64 characters in both ACLI and EDM.
wi01004362	Security 802.1X EAP: In a scenario where an IP Phone and a PC behind the phone are connected into an EAPOL multihost enabled port and only the IP Phone is successfully authenticated, starting a ping over IPv6 into the system's management VLAN's IPv6 address will succeed even if the PC is not successfully authenticated. However, all other IPv4 and IPv6 traffic not destined for the switch will be dropped.

Change Request number	Description
wi01028882	SMLT/LAG: Currently in an SMLT over LACP scenario, the ACLI environment allows entering commands for binding multiple LAGs to the same SMLT ID. However, only one (the first one configured) binding becomes actually operational. Avaya recommends that you keep the LAG to SMLT ID bindings as one-to-one in order to avoid creating ambiguous device configurations.
wi00945013	SNMP: SNMP inform traps are not generated correctly by the switch (both header and PDU variable bindings) and will fail to be interpreted by the receiving SNMP trap daemon host.
wi00962526	AAUR: When carrying out the AAUR process in a pure Waverunner stack, the message `NVR CFG - Could not acquire FLASH sem` will be registered throughout all units of the stack. There is no impact on the AAUR process which will be successful.
wi00925548	DecOtherEther2, Filter Limiting: When Filter Limiting is disabled and configured to use additional filter slots (beyond 7), the saved ASCII configuration will include the additional VLANs which are defined using the extended filter slots. If a switch/stack is reset to defaults, it will come up with Filter Limiting enabled and will now be limited to 7 filter slots. VLANs which are defined for the additional slots will fail to be configured on the switch. The use of a DecOtherEther2 protocol VLAN will fail since it requires 10 protocol slots. If a configuration is using the slots provided by disabling filter limiting, you must disable filter limiting via ACLI and reboot the switch/stack before applying the ASCII configuration so that it is operating in the Filter Limiting disabled mode.
wi00930131	SLPP Guard: The ACLI command **`no slpp-guard`** disables slpp-guard on a specific port **`(no slpp-guard port X enable)`** or disables the auto re-enable timeout **`no slpp-guard port X timeout)`**. If neither parameter is specified (**enable** or **timeout**), both settings will be disabled, i.e. slpp-guard is disabled and the timeout set to 0 on the specified port(s).
wi00987107	EDM, Rate Limiting: When configuring rate-limit settings for switch ports using EDM, setting pps or percent for either the broadcast or multicast traffic type will trigger the both parameter to apply for the port selection.
wi01016205	When initiating an eapol init on a port with authenticated EAPOL users that have associated DHCP-clients leases that populate the dhcp-snooping binding table, users will be de-authenticated but former entries may still populate the dhcp-snooping binding table. You can issue a manual clear mac-address table command.
wi01021166	MLT, MAC Security: When using MLT trunk ports with MAC-Security auto-learning and a set threshold (for example 20 out of 25 maximum possible value), bouncing the MLT trunk from enabled state to disabled

Change Request number	Description
	state several times may cause the MAC SA entries learned to exceed the threshold.
wi00945962	VRRP: If you encounter the message `% Not enough HW resources available` when enabling VRRP, try again after a 30 second interval. This may result from high CPU utilization.
wi01030857	MAC Security, EDM: The MAC-Security "MacViolation" tab from EDM will not list any intruder mac-addresses as expected.
wi01039420	Voice VLAN: If you encounter an Invalid Voice-VLAN ID error message while attempting to enable ADAC on a standalone switch which used to be part of a stack (even if the voice VLAN is set) check that the VLAN is a voice VLAN with command **`show vlan voice-vlan`**. If the VLAN does not appear in the list of voice VLANs, issue the command **`vlan voice-vlan vlan_id`** to enable ADAC.
wi01035284	LACP and mrouter ports are mutual exclusive. Avaya recommends using mrouter ports with MLT.
wi00973591	Even though the image has been downloaded successfully and the continuous ping was not interrupted the following messages are displayed intermittently : `Request time out!` The connection with the device may be lost or the device may be down.
wi00974433	RADIUS key for secondary servers (GRS/ERS/NRS) is deleted when defaulting primary server. Is recommended to use "no radius server host" instead of "default radius server host". This way, if a secondary server is configured, the key will remain in use for that secondary server.
wi00973591, wi00975529	RADIUS dynamic server clients statistics may not be seen when using EDM Offbox.
wi00936876	OSPF, SMLT: An intermittent error may be seen when OSPF over SMLT is configured in a looped environment (SLPP enabled).
wi00978991	EDM, BGP: When creating a community list or As path list from EDM, with member id greater than 10, the list will not be displayed correctly from EDM.
wi00984496	EDM System up-time: Stack info uptime seen from EDM does not display uptime for non base units.
wi00989413	EDM, Stack Health: Display of switch stack health in EDM after units in stack are renumbered may not be accurate. **Workaround**: use ACLI command.
wi00992210	MAC Security address table: Static entry in the MAC security table should be created before planning to remove unit from stack.

Change Request number	Description
wi00993182	EDM, LACP: In EDM, sorting the trunks in the Vlan->MLT/LACP section is possible only for the MLT tab.
wi01004253	EDM, stack information: The display of stack information in EDM after booting the base unit may not be correct. ACLI should be used.
wi01005364	DHCP, reboot: After reboot, DHCP requests from client pass the switch port before MAC authentication(radius-request) starts. The device receives an IP address of the Guest VLAN , even if the client is eventually authenticated and moved to initial / radius vlan .This scenario is reproducible only when clients are simulated by traffic generators; the issue is not reproducible in a real case scenario (client = PC / IP Phone)
wi01008960	EAP: If no more than 4 minutes and 30 seconds have passed after an EAP user is authenticated , a flush of the mac address table on the switch/stack will have no effect on the user`s authentication . However , if this timer expires , the client will try to re-authenticate and if it is still there it will get re-authenticated.
wi01013703	EDM, IST: IST may not be enabled when EDM is used. Workaround: Enable IST from ACLI.
wi01018390	COM: The following message is displayed, even though the connection is not lost. `Request time out!` The connection with the device may be lost or the device may be down.
wi01019181	The management traffic might be affected in a case where a static IPv4 route used for switch management from a remote network is more specific than a local route. To reestablish the management connection, the configuration of an IPv4 management route for the same network is required
wi01021894	LLDP: In version 6.3, the LLDP default settings for lldp tx-tlv and lldp tx-tlv med have been changed to enabled. In prior releases, the default setting for LLDP was disabled. These settings only apply when the switch is defaulted or the default LLDP setting is applied. When upgrading from a previous version, the configured LLDP settings will be retained.
wi01022088	EDM, MSTI: The error message `inconsistentValue` is displayed when trying to create an MSTI which already exists.
wi01022549	When the device reaches a situation in which it sends out an ICMP Destination Unreachable message through a specific port, the icmpOutDestUnreachs.0 counter should be increment each time such a message is sent. Currently this counter is not incrementing properly so it is best to rely on capturing such packets if required for a traffic statistic.

Change Request number	Description
wi01024984	The error message `% TFTP server address has not been set` is intermittently displayed for the command `configure network`.
wi01027416	SNMP: The error message `commit failed` is returned when a user tries to disable the STG of the management VLAN using SNMP.
wi01027752	Multicast traffic might be lost after maximum of multicast routing entries(992(*,G)and(S,G)) are learned on WR stacks.
wi01028882	SMLT over LACP: Currently in a SMLT over LACP scenario the ACLI environment allows entering commands for binding multiple LAGs to the same SMLT ID. However, only one (the first one configured) binding becomes actually operational. Avaya recommends that you keep the LAG to SMLT-ID bindings as one-to-one in order to avoid creating ambiguous device configurations.
wi01028979	PIM: The command `show ip pim interface enabled` may not return any of the enabled pim interfaces after a reset of the device.
wi01034689	EAP/NEAP, RADIUS: Using EAP/NEAP users with RADIUS assigned VLAN and fail open VLAN, authenticated users use RADIUS assigned VLAN. If the RADIUS server is unreachable, clients are moved in fail open VLAN. After defaulting to the RADIUS server, users are removed from fail open VLAN, while remaining authenticated. They will use RADIUS assigned VLAN. Reauthentication is not performed in this situation (EAP and NEAP clients are not flushed).
wi01035281	SMLT: Avaya recommends that you refrain from consuming all of the trunks 1-32 since configured aggregated trunks will utilize these starting at 32 and progressing through lower numbers (31, 30, 29, ...). Trunks may be configured using values of 33-512 and not create any conflict with trunks formed by aggregation.
wi01035500	Brouter, IGMP Snooping: ip igmp snoop is not supported on brouter port. However, no error is returned when configuring it.
wi01035841	SLPP: If the '0' option is selected from the output of the `slpp timeout` command, the slpp timeout will be set to '4'.
wi00931239	EDM, Rate-limit: When configuring rate-limit from EDM on a multiple port selection, desired values may sometimes not be applied as expected. The same options can be set from ACLI.
wi00980212	OSPF, MAC security: Avaya recommends you do not use MAC security on OSPF enabled links on 5520 and 5530 units.
Known Issues from Release 6.2	
wi00484542	In an NSNA setup, you may experience temporary loss of NSNA functionality when UDP forwarding has approached maximum

Change Request number	Description
	capacity. Workaround: Configure a filter on the port that connects to the SNAS (or depending on your configuration, on the port connected to the switch that, in turn, connects to the SNAS) to isolate NSNA SSCP traffic received by the CPU. Use the following CLI commands to configure a filter: **qos ip-element <element_id> src-ip <ip_address/mask>** **qos classifier <value> set-id <value> element-type ip element-id <value>** **qos action <value> update-1p <value>** **qos policy <value> port <port_list> clfr-type class clfr-id <value> in-profile-action <action_id> prec <value>**
wi00486525	VRRP may intermittently bounce when multiple protocols are configured on upstream routers with traffic and large routing updates.
wi00486579	Inconsistent display of pluggable modules in BigWave Stacks.
wi00486677	It may take more time than usual for traffic to re-converge (approximately 10 seconds) if a stack from the core is rebooted in a highly scaled SMLT configuration (100 VLANs).
wi00494404	Port mirroring mode XrxYtx on a 56XX device does not mirror broadcast, multicast and unknown unicast traffic if the X and Y mirrored ports are in different MLTs.
Q01979384-01	HTTP connections are not displayed by the **show ipv6 tcp connection** command.
wi00486987	PM Unicast doubled on monitor - hybrid stack, using xRx Or/And yTx. modes.
wi00486821	The **show ip ospf neighbor detail** command that provides detailed information for OSPF LSDB should not be run when the terminal length is set to 0.
wi00494658	A non-PoE phone may display as Unknown and need to be rebooted after a stack is rebooted.
Q02004055	There is currently no command to disable the **metric** and **route-type** options for the **route-map <route_name> match** command and no command to disable the **ip preference**, **metric**, and **metric-type** options for the **route-map <route_name> set** command.
wi00486751, wi00490844, wi00497003	When the maximum of 10 DHCP clients are bound by IP Source Guard on MLT/LACP ports, if those ports go down, several IPSG binding table full messages will be logged. This is an incorrect behavior.

Change Request number	Description
wi00486734	On a stack with 55xx units with all QoS filters or masks used, when ADAC tries to use another QoS mask / filter (unavailable because of exhausted resources), the system displays a **`commitFailed 1`** message. The correct message is displayed for a 56xx or 55xx standalone device.
wi00494595	Specifying a range of ports for non-base units using the **`poe poe-shutdown port X`** command may cause IP Phones connected to those ports to remain powered on in some stack configurations.
wi00486898	Wait twice the configured MAC aging time after swapping two PCs behind 2 phones in an NSNA solution before plugging the PCs back in behind the phones.
wi00482532, wi00487440, wi00497112	IPv6 traffic not destined for the switch or stack will not be processed by ERS 5500 Series units and therefore IPv6 neighbor cache entries will not be created for the devices exchanging traffic. This behavior is different on ERS 5600 Series units where entries are created if traffic passes them. In either instance the actual flow of IPv6 traffic is not influenced, just the contents of the neighbor cache.
wi00494935	If the UBP set is configured and the QoS agent is disabled when an EAP / Non EAP user authenticates, several log messages displaying **`QoS support is currently disabled`** will be produced.
wi00487438	OSPF: Even though two LSA packets are sent (one with unicast destination address and one with multicast destination IP) only one LS ACK transmitted packet appears in the interface statistics table.
Q02056133-02	EDM: to enable or disable EDM access use ACLI commands **`web-server enable`** or **`web-server disable`**.
wi00495084	STP is re-enabled when moving SMLT ports from 1 STG to another.
wi00484360, wi00487405, wi00497106, wi00554983	Stacking: When you copy a binary configuration to an TFTP server, you may receive an `Intra-stack communication failure` message. This does NOT indicate a stack failure; it indicates that the command failed. **Workaround**: : If you receive the `intra-stack communication failure` message, execute the **`copy binary`** command until it succeeds.
wi00487763, wi00494841, wi00498010	STACKING, NSNA: In a stack with a large number of NSNA-enabled ports, a great deal of inter-unit messaging related to NSNA filter installation occurs at start-up. In some circumstances, processing of these messages may be delayed long enough for the message originator (typically the base unit) to consider the messages lost and an error to have occurred. However, message processing on the non-base units may have completed successfully after a minimal delay, allowing NSNA configuration to successfully complete. In this case, errors included in the system log may not signify actual configuration errors. If you receive error messages but suspect that NSNA

Change Request number	Description
	configuration is complete, examine the NSNA-enabled ports to determine whether they correctly configured. If you find discrepancies, disable and re-enable NSNA.
wi00495158	In the SMLT network, loop may be temporarily introduced on LACP-over-SMLT port. In order to prevent loop from happening it is required to configure all LACP-over-SMLT port in "Lacp Advance mode". Under this mode, LACP port stays in Blocking mode until it receives the first LACP PDU from its partner port. In 6.2 release, it is the user's responsibility to put all LAC-over-SMLT ports in "Lacp Advance Mode.
wi00488453	Do not see the ability to set Forced Stack Mode via the EDM interface.
wi00495698	SFPs: To ensure a proper match of the remote side, before you install an SFP set shared ports to auto-negotiate. Refer to ACLI: default speed and default duplex
wi00495332	IPv6 Tunnel over IPv4 operational status is determined by combination of IPv6, IPv4 forwarding, and VLAN status. The IPv6 tunnel operational status is ACTIVE if IPv6, IPv4 forwarding is enabled and the VLAN status to which source IPv4 tunnel end point is UP (i.e. at least one port on VLAN is connected). Operational status ACTIVE does not indicate the liveliness or reachability of IPV4 remote tunnel end point.
Q02089575	Supported capabilities in Ethernet Routing Switch 5000 Series switches, the maximum supported PIM-SM entries should state up to 492 for 55xx Switches and up to 992 for 56xx Switches - not 500 and 1000.
wi00484056, wi00487793, wi00497158	TDR: Run TDR tests only for ports with Link Status UP.
wi00487998	**Demo Licens**e: If you use a Demo License and you remove the Demo License, you must reboot the stack.
wi00484096, wi00488154, wi00497196	`show running-config defaults` When you execute the show running-config defaults or show running-config default specific commands the system may take up to 4 minutes to return results, depending on the complexity of the system: for example, an 8-high stack fully configured. This is considered normal behavior.
wi00496125	The old RSTP Traps command is hidden (this means is not displayed when question mark is given and the command is not autocompleted when hitting TAB). Use the new commands found under 'snmp-server notification-control'. You can obtain a list of the current notification traps available using 'show snmp-server notification-control'.

Change Request number	Description
wi00487670	IPv6 DHCP Relay does not support Remote ID parameter (RFC 4649) in this release.
wi00488121	EDM, RATE LIMITING: Multiple port configuration for Rate Limiting may not work properly; the change allow rate of broadcast or multicast may produce an incorrect result. WORKAROUND: Use ACLI to configure Rate Limiting.
wi00495711	In Lossless mode, when oversubscription exceeds 10 ports to 1 port, ingress ports must be spread across groups of 24 ports.
wi00496306	Energy Saver: When energy saver is activated or deactivated, the link on a port briefly transitions. This causes some devices to re-acquire connectivity. For copper uplink ports or critical devices, it is recommended to disable energy saver at the port level.
wi00496308	EAP authentication will be restarted on copper ports when Energy Saver transitions to active or inactive state. This occurs because Energy Saver is clearing the MAC address on the EAP client port when transitioning to the active or inactive state. EAP fiber port status does not change when Energy Saver is activated or deactivated.
wi00496309	NEAP authentication is restarted on copper ports when Energy Saver transitions to active or inactive state. This occurs because Energy Saver transition clears the MAC address on the NEAP client port. NEAP fiber ports EAP status does not change when Energy Saver is activated or deactivated
wi00487721	PORT MIRRORING: Port mirroring will mirror pruned multicast streams to the monitor port. However, the streams are not actually sent to the device because they are pruned.
wi00488227	EDM, Multiple Port Selection: EDM can delete up to a maximum of 120 ports when you use multiple port selection. If you select more than 120 ports, some of the ports may not disabled.
wi00495772	NSNA: When you use an NSNA configuration on multiple units from a stack, after boot some NSNA errors may be present in the logs. NSNA will work as expected even if these errors are present.
wi00488679	EDM: You cannot view and configure 802.1ab Dot1 settings for Local Protocol Vlan and Local Vlan Name using EDM. **Workaround**: Use ACLI to view and configure 802.1ab Dot1 settings for Local Protocol VLAN and Local VLAN name
wi00555143	Upgrade: All trap notifications are enabled after you upgrade to R6.2.0 software, regardless whether you disabled them prior to the upgrade. For procedures to restore trap functionality, see Trap restoration and reconfiguration after upgrade to Release 6.3 on page 53.
wi00496317	ROUTING, DEFAULT GATEWAY: If you enable and disable routing globally on the management VLAN the default gateway may not work. In R6.2 you can configure the switch with default gateway (using the

Change Request number	Description
	command **ip default-gateway <next-hop>** or default route (using the command **ip route 0.0.0.0.0.0.0.0 <next-hop>**). When IP Routing is disabled (Layer 2 mode) on the switch, the default gateway serves as the default route, that is the default gateway shown by the **show ip** command. When IP Routing is enabled (Layer 3 mode) on the switch, the default route specified is used, that is the 0.0.0.0 route shown by the **show ip route** command. You can enter up to 4 static routes, management static routes, to be used for management traffic only. These routes are used in software routing only and do not affect pure data plane traffic. SOLUTION: You must enable routing on the management VLAN to activate management static routes which you can use for separation of management and data traffic.
wi00488714	LLDP MED NETWORK POLICIES: You cannot assign custom DSCP values to Avaya 1120E IP Deskphones using LLDP MED network policies.
wi00491740, wi00496258, wi00498185	It is recommended that you use SNMPv3 to achieve security, instead of using SNMPv1 and/or SNMPv2c with community strings.
wi00554963	RADIUS, RADIUS reachability: If you use the "radius reachability use-radius", the switch sends reachability requests with the username ’avaya’ and a blank password. Because the Avaya ignition server does not allow accounts to be created with a blank password, the ignition server will log intrusion events when the dummy requests are regularly sent from the switch. WORKAROUND: Use ICMP reachability for ignition server reachability.
wi00554875, wi00555204, wi00555283	802.1ab MED: Both LLDP MED and ADAC policies are supported on the same port. If both types of policies are created on the same port and you delete the LLDP policy you created, then the ADAC policy is also deleted.
wi00554955	IPv6 Static Routes: In an IPV6 setup where static and backup static routes exist, if you disable the IPv6 routing on a neighbor next-hop router, the active route will remain active until ARP for the next-hop expires or until a neighbor solicit message is forced (ping, clear neighbor, clear neighbor mac address) or until you execute shutdown/ noshutdown on the respective interface.
Q02149708	Energy Saver: You must not select fiber ports when you use the Multiple Port Configuration menu to enable Energy Saver on a range of ports.
wi00555215	EDM, MSTP: If your environment contains a large number of stacks and a large number of ports and you click between the CIST Port, MSTI

Change Request number	Description
	Bridges, and MSTI Port tabs, the system may display the Unresponsive script dialog because you have initiated a large data retrieval.
Q02150634	AUR/DAUR: The reboot process can take approximately 3 minutes to complete, after which the normal CLI commands will display the AUR status.
wi00555132	AUR, LICENSING: After you perform automatic unit replacement (AUR) of a base unit, if the MAC address of the new unit introduced into the stack was not part of the original license, then, when you reboot the stack and execute the ACLI command **`show license all`**, the output displays that 0 licenses are present. WORKAROUND: Licenses will be operational, or can be enabled, and you can verify the license state using the following ACLI commands: • **`show license all verbose`** to check whether any bit is set in the License Vector in Use data • **`show sys-info`**: the Operational license field shows the current license state • **`show system verbose`**: Operational license field shows the current license state
wi00555156	SLPP: In a stack of 5 or more units that runs a complex configuration, for example, SMLT, LACP, SLPP, or OSPF, SLPP can fail to detect and prevent loops due to inadequate system resources. SLPP PDUs are not treated as high priority packets and are not processed on time. This does not happen on SLPP ports on the base unit.
wi00933491	802.1AB MED network policies: Avaya IP phones may not apply LLDP MED network policy configurations received from the switch on older phone firmware versions.
wi01008592	LLDPDU and TLV error handling: in the scenario where you have a large number of VLANs configured and dot1 port-protocol-vlan-id and vlan-name TLVs are enabled, TLVs may not be transmitted. With the maximum size of an LLDPDU packet at 1518 bytes, some TLVs such as dot3, MED, and vendor specific Avaya TLVs may not be sent.
wi00934940	LLDP Integration: on the Avaya IP phones, the Current Conservation parameter is not set according to the PoE conservation level request TLVs.
wi00834482	When LACP and SLT's are configured IST's, some SLT ports may blocked traffic. If this happens, bouncing the SLT ports on the IST peers where the block occurs should resolve the issue and traffic can be seen forwarding again. This issue will address in the maintenance build.

Trap restoration and reconfiguration after upgrade to Release 6.3

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

Restoring trap notification functionality using ACLI

About this task

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

Procedure

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

Reconfiguring traps using EDM

About this task

Use the following procedure to reconfigure traps using EDM:

Procedure

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

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

About this task

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

Procedure

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

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

   Enter community string: CommunityName

   Enter community string: CommunityName

2. To create an SNMP host using the community you created in the previous step, from the Global Configuration prompt enter the following command: `snmp-server host 10.100.68.3 port 162 v1 CommunityName filter TestFilter`.

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

About this task

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

Procedure

1. To create an SNMP community, from the Global Configuration prompt, enter the following command: `snmp-server community CommunityName notify-view nncli`.
2. To create an SNMP host using the community you created in the previous step, from the Global Configuration prompt enter the following command: `snmp-server host 10.100.68.3 port 162 v1 CommunityName filter TestFilter`.

Setting the Notification Type per receiver using ACLI

About this task

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

Procedure

1. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter +org`.
2. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter -linkDown`.
3. From the Global Configuration prompt, enter the following command: `snmp-server notify-filter TestFilter -linkUp`.

Displaying Notification Types associated with the notify filter using ACLI

About this task

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

Procedure

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

Enabling or disabling the Notification Type per device using ACLI

About this task

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

Procedure

1. From the Global configuration prompt, enter the following command: `no snmp-server notification-control linkDown`.

2. From the global Configuration prompt, enter the following command: `no snmp-server notification-control linkUp`.

Preventing a loop during upgrade of a large network

About this task

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

Procedure

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

Ethernet Routing Switch 5000 Series limitations and considerations

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

Table 5: Ethernet Routing Switch 5000 Series considerations

Item	Description
1	Some terminal programs can cause the Console Interface to crash if you enter a RADIUS secret containing the character “k”. The issue has been reproduced using Tera Term Pro (version 2.3), as well as Minicom (version 2.1) on a Linux system.
2	Avaya recommends that you avoid using MAC security on a trunk (MLT).
3	Failed attempts to log in (using TACACS+ authentication and accounting) are not stored in the accounting file.

Item	Description
4	When switches are in MSTP mode and connected using a trunk (MLT), and at least one MSTI is configured, the switch can return an incorrect STPG root if you change the mode to STPG and reset the switches.
5	When you use the JDM/Web to configure and add VLAN ports to an STG other than the default STG, STG membership of the port may change. In that case, the new STG participation of that port will be disabled. WORKAROUND: Enable participation of the ports in the new STG after you enable the STG.
6	On the 5530-24TFD, the following (NT-OCP) SFPs cannot be inserted side by side (that is, in neighboring slots) because of the SFP size. For a list of SFPs, see SFPs that cannot reside in neighboring slots in the ERS 5530-24TFD on page 59.
7	While downloading the image file, you may receive the following error message: "Error reading image file." WORKAROUND: Typically, this issue can be resolved by simply restarting the image download. If this does not resolve the issue, Avaya recommends that you try an alternate method to download the image to the switch (that is, the Web Interface).
8	The IPFIX sampling data rate cannot be changed because of a related hardware limitation.
9	Release 5.1 introduced a Demo License to enable OSPF, ECMP, VRRP, SMLT, and IPFIX for a period of 30 days. The trial license expires at the end of the 30-day period and the features, except SMLT, are disabled. The system sends traps advising of license expiration but SMLT remains enabled until the stack or unit is reset. Avaya recommends that, when you receive the first trap, the administrator begins to manually disable SMLT and ensure removal of any cabling loop. Because Spanning Tree Protocol needs to be disabled and, because SMLT is implemented through cabling, SMLT is not disabled with the other features because a network loop would form. After demo license expiry, when the stack or unit is reset, SMLT is disabled and a loop will form if there has been no intervention to remove or disable the ports participating in the IST. Demo license expiry traps: Five days prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 5 day(s). One day prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 1 day(s). At termination of demo license: bsnTrialLicenseExpiration: Trial license 1 has expired.
10	When you configure IPFIX to work with NetQoS, Avaya recommends that you disable the SNMP polling by NetQoS device. To do this, remove the community string associated with the ERS 5500 Series switch on NetQoS device.
11	Avaya recommends that you do not enable IP Source Guard on trunk ports.
12	Avaya recommends that you do not enable Critical-IP functionality with VRRP in an SMLT environment.

Item	Description
13	Lossless Mode: Lossless activates in oversubscription scenarios even if rate-limiting is applied to certain ingress streams and slowing them is not necessary. Lossless gives fair access to bandwidth, meaning that if you have 3 ingress streams of 100% line rate competing on 1 egress port, lossless will slow down the sender transmit rates to a 33-33-33 percentage, and it does this by sending pause frames. If you have 2 streams coming in at 100% and a third at 20%, lossless will not interfere with this stream, the egress percentages will be 40-40-20. If the third stream transmit rate exceeds 33%, lossless will begin to apply to it as well. In this situation, if applying a meter to this stream, limiting it at under 33%, lossless doesn't activate and doesn't interfere. However, if the third stream is either broadcast or multicast traffic and a rate-limiting setting is applied instead of a meter, lossless will activate - it will send pause frames to the sender. The egress rate of the stream is not affected, it will be the one imposed by the rate-limiting setting, but the transmit rate will vary because of the pause frames.
14	Lossless Mode: In Lossless buffering mode, if you use ingress traffic with queue 1 + ingress traffic with queue 2, and the egress port is on a different asic from ingress ports, QoS queue shaper may limit the bandwidth for queue 1 under the min-rate and egress traffic may be under the expected rates.
15	ARP Table Size for ERS 5600: The maximum number of entries in the ARP table is 2500 for a pure stack, and 1500 entries with a hybrid stack.
16	MAC Filtering List: Release 6.3 of ERS 5000 increases the maximum number of entries in the MAC Filtering List to 128. More upper limit testing is required.
17	Inexistent VLAN Mapping for MSTI: EDM/SNMP support for VLAN Mapping for MSTI is not available in Release 6.3.
18	In Release 6.3, the LLDP default settings for lldp tx-tlv and lldp tx-tlv med have been changed to enabled. In prior releases, the default setting for LLDP was disabled. These settings only apply when the switch is defaulted or the default LLDP setting is applied. When upgrading from a previous version, the configured LLDP settings will be retained.

19	You cannot enable MAC Security on LACP enabled ports. The following message displays:
	`%Cannot modify settings`
	`%MAC Security status cannot be modified. Disable LACP first.`

20	Rate Limiting: When you have the following scenario: 1. rate-limiting is performed at 10% (or by setting any percent value threshold) 2. the speed ratio between the inbound port and the client port is 10:1 (for example 10Gbps inbound link and 1Gbps client port link) 3. inbound broadcast or multicast traffic throughput on the inbound link is more than 10% link-rate speed

Item	Description
	then the client port will receive 0.1 * [inbound traffic rate] and not the expected 1Gbps broadcast or multicast traffic. Example: • inbound port link rate = 10Gbps , client outbound link rate = 1Gbps , rate limiting set to both at 10% • inbound traffic rate = 3Gbps broadcast traffic The actual client traffic received rate = 333Mbps and not the expected 1Gbps
21	In a stack configuration, SSHC configuration options are only available from the base unit

22	When you manually create an LLPD MED network policy, LLDP checks that the specified VLAN ID corresponds to a voice VLAN created inside the VLAN application. If the VLAN is not a voice VLAN or the VLAN does not exist, the switch displays a warning message. The switch creates the policy even if the VLAN is not voice enabled or does not exist. The switch may display one of the following messages:
	`% Policy will be set on port x with vlan-id of a non-existent vlan y`
	`% Policy will be set on port x member of the non-voice vlan y`

SFPs that cannot reside in neighboring slots in the ERS 5530-24TFD

The following list of SFPs states the manufacturer’s part number and Avaya part number for SFPs that cannot reside in neighboring slots in the ERS 5530-24TFD.

- TRP-G1H5BC470N4 / AA1419025
- TRP-G1H5BC490N4 / AA1419026
- TRP-G1H5BC510N4 / AA1419027
- TRP-G1H5BC530N4 / AA1419028
- TRP-G1H5BC550N4 / AA1419029
- TRP-G1H5BC570N4 / AA1419030
- TRP-G1H5BC590N4 / AA1419031
- TRP-G1H5BC610N4 / AA1419032
- TRP-G1H7BC470N4 / AA1419033
- TRP-G1H7BC490N4 / AA1419034

- TRP-G1H7BC510N4 / AA1419035
- TRP-G1H7BC530N4 / AA1419036
- TRP-G1H7BC550N4 / AA1419037
- TRP-G1H7BC570N4 / AA1419038
- TRP-G1H7BC590N4 / AA1419039
- TRP-G1H7BC610N4 / AA1419040

VLACP issue

In some situations, when you use VLACP the ERS 5000 series switches remove a link from service due to variations in the arrival time of VLACP messages (VLACP PDUs) from the far end. The issue can exist between the ERS 5500 and ERS 5600 models and ERS 8300 and ERS 8600 models when the system runs short timers with a default timeout interval of 3 time-outs or less. The ERS 5500 and ERS 5600 switches maintain a rolling history of the last 3 received VLACP PDUs (by default) and calculate the time variance across and between these VLACP messages.

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

Port or ifIndex offset issue

If you use Software Release 6.0, specify switch_type ERS5500 at the SNAS for standalone switches or stacks.

Filter resource consumption

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

A filter specifies the bit pattern to match.

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

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

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

Table 6: Application mask and filter resource requirements

Application	Category	Masks required	Filters required
Ethernet Routing Switch 5500 Series			
QoS (Auto QoS)	QoS	1	4
IGMP	Non QoS	2	10
Port Mirroring (MAC-based)	Non QoS	2	2
EAP Authetication (EAPoL packet filter)	Non QoS	1	1
BaySecure (ERS5520/30 only)	Non QoS	1	32
EAP MHMA Allowed Clients (5520/30)	Non QoS	1	32
IPFIX	Non QoS	1	1
QoS Interface Applications	QoS	17	17
NSNA MAC Intruder	Non QoS	1	32
NSNA (R/Y/G filters)	QoS	5	8
ADAC	Non QoS	1	1
RIP	Non QoS	1	1
UDP Broadcast	Non QoS	1	1
VRRP	Non QoS	1	1
OSPF	Non QoS	1	1
IP Source Guard	Non QoS	1	10
Ethernet Routing Switch 5600 Series			
Broadcast ARP and ARP Inspection	Non QoS	1	1
DHCP Relay or DHCP Snooping or NSNA DHCP	Non QoS	1	2
QoS (default untrusted policy)	QoS	2	2
QoS (DAPP with status tracking)	QoS	1	1
QoS (Auto QoS)	QoS	1	4

Application	Category	Masks required	Filters required
Port Mirroring (MAC-based)	Non QoS	1	2
EAP Authetication (EAPoL packet filter)	Non QoS	1	2
IPFIX	Non QoS	1	1
NSNA MAC Intruder	Non QoS	1	32
NSNA (R/Y/G filters)	QoS	5	8
ADAC	Non QoS	1	1
RIP	Non QoS	1	1
UDP Broadcast	Non QoS	1	1
BGP (ERS 5600 only)	Non QoS	1	2
VRRP	Non QoS	1	2
OSPF	Non QoS	1	2
Content Based Forwarding (ERS 5600 only)	Non QoS	1	1
IP Source Guard	Non QoS	1	11
PIM	Non QoS	1	1

On the ERS 5500 Series switches 16 masks and 128 filters are available on each port. By default, 2 masks and 2 filters are consumed by the system for ARP filtering and DHCP relay, leaving 14 masks and 126 filters available to QoS and other non QoS applications to configure dynamically.

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

You can use the **`show qos diag`** command to assess the current filter resource usage for each port on ERS 5000 Series switches.

The **`show qos diag`** command displays the number of QoS masks and filters and non QoS masks and filters consumed on each port. You can determine whether an application that requires filter resources can be enabled on a port by verifying that the number of available masks and filters meets the mask and filter requirements of the application.

On ERS 5500 Series switches, the available masks and filters on a port can be determined by adding the total number of QoS and non QoS masks in use and the total number of QoS and non QoS filters in use on a port, then subtracting that number from 16 masks and 128 filters.

On the ERS 5600 Series switches, you can count the unused masks to determine the number of available masks for a port by using the output of the **`show qos diag`** command. The ERS 5600 Series switches share resources across a group of ports. The filters used by QoS or non QoS applications on a port for a specific mask determine the available filters for that mask for all ports from that group.

On the ERS 5600 Series switches, you can determine the number of filters available for a mask from a group of ports by adding the total number of QoS and non QoS filters in use and subtracting that number from 256. If the number of filters in use for a mask equals 256, you cannot use that mask on other ports from the same group.

Example — IP Source Guard on an ERS 5500 Series switch port

On ERS 5500 Series switches, you need 1 mask and 10 filters to enable IP Source Guard on a port. When you view the show qos diag command out you see that port 5 is currently using a total of 4 masks and 5 filters. This means that 12 masks and 123 filters are available for use. So you can enable IP Source Guard on port 5.

Example - IP Source Guard on an ERS 5600 Series switch port

On ERS 5600 Series switches you need 1 mask and 11 filters to enable IP Source Guard on a port. When you view the show qos diag command output you see that port 5 is currently using a total of 4 masks. IP Source Guard uses the next available mask and, from the command output, you can see that there are 256 filters available for mask 14. So you can enable IP Source Guard.

QoS Interface Security Application

The QoS Interface Security application only runs on ERS 5500 Series switches. It targets a number of common network attacks. Support includes ARP spoofing prevention, DHCP snooping, DHCP spoofing prevention, detection for the common worms SQLSlam and Nachia, and the Denial of Service (DoS) attacks Xmas, TCP SynFinScan, TCP FtpPort, and TCP DnsPort. Due to the lack of filter resources (masks) to enable the whole QoS Interface Security application, you can select individual security applications.

The following table summarizes the mask and filter resource requirements for individual QoS Interface Security applications.

Table 7: Mask and filter resource requirements

QoS Interface Security Application	Masks required	Filters required
ARP Spoofing Prevention	5	5

QoS Interface Security Application	Masks required	Filters required
DHCP Snooping	1	1
DHCP Spoofing Prevention	2	2
DoS SQL Slam	1	1
DoS Nachia	1	1
DoS Xmas	1	1
DoS TCP SynFinScan	1	1
DoS TCP FtpPort	2	2
Dos TCP DnsPort	2	2
QoS BPDU blocker interface	1	1