Avaya Ethernet Routing Switch 3500 Series Release Notes

5.0
NN47203-400
01.01
May 2012

Contents

Chapter 1: Purpose of this document

This document describes new features and important information about the latest release. Release Notes includes a list of known issues (including workarounds where appropriate) and a list of fixed issues.

Chapter 2: New in this release

This is a new document for Avaya Ethernet Routing Switch 3500 Series Release 5.0.

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

Hardware

The following table lists and describes supported hardware for the Avaya Ethernet Routing Switch 3500 Series Release 5.0. Question marks (?) in the table signify power cord types; substitute the following regional variants:

- A — no power cord
- B — EU power cord
- C — UK / Ireland power cord
- D — Japan power cord
- E — North American power cord
- F — Australia / New Zealand / China power cord

Table 1: Hardware

Hardware	Description
Switch models	
AL3500?01–E6	3526T — 24 10/100BaseT ports supporting autosensing, autonegotiation and autopolarity, in a non-PoE , plus two 10/100/1000 or Small Form Pluggable (SFP) front combination ports, plus two SFP rear ports. Fanless.
AL3500?11–E6	3526T-PWR+ — 24 10/100BaseT PoE+ ports (802.3af/at), plus two 10/100/1000 or Small Form Pluggable (SFP) front combination ports, plus two SFP rear ports.
AL3500?04–E6	3510GT — 8 10/100/1000BaseT ports, plus two SFP ports (ports 9 and 10). Standalone and fanless.

Hardware	Description
AL3500?14–E6	3510GT-PWR+ — 8 10/100/1000BaseT PoE + ports (802.3af/at), plus two SFP ports (ports 9 and 10). Standalone. Fanless operation in Low Power mode @ 60W max PoE budget, or normal fan operation in High Power mode @ 170W max PoE budget.
AL3500?05–E6	3524GT — 24 10/100/1000BaseT ports, four SFP ports shared with ports 21–24, plus two SFP rear ports.
AL3500?15–E6	3524GT-PWR+ — 24 10/100/1000BaseT PoE+ ports (802.3af/at), four SFP ports shared with ports 21–24, plus two SFP rear ports.
Rack Mount Kits	
AL3511001–E6	Spare Rack Mount Kit — this kit can be used as a replacement rack mount kit for ERS 3524GT, ERS 3524GT-PWR+, ERS 3526T or ERS 3526T-PWR+ switches.
AL3511002–E6	3510–Pair Rack Mount Kit — this kit is used to connect two ERS 3510GT or ERS 3510GT-PWR+ switches together side by side and mount them in a 19 inch rack.
AL3511003–E6	3510–Single Rack Mount Kit — this kit is used to mount a single ERS 3510GT or ERS 3510GT-PWR+ switch in a standard 19 inch rack.

Features

The following sections highlight the feature support provided in Release 5.0.

256 port-based VLANs with IVL

In Release 5.0, the Avaya Ethernet Routing Switch 3500 Series supports 256 VLANs, either by port, under the 802.1d bridging model, or IPv6 protocol-based VLANs. When the Avaya Ethernet Routing Switch 3500 Series is installed for the first time, all ports are assigned to the default VLAN (PVID=1). The default management VLAN is VLAN 1.

Avaya Ethernet Routing Switch 3500 Series supports the Independent VLAN Learning (IVL) model. IVL allows duplicate MAC addresses to be present in different sets, but not in the same set or VLAN. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

802.1AB and ADAC interoperability

Avaya Ethernet Routing Switch 3500 Series supports Auto-Detection and Auto-Configuration (ADAC) of Avaya IP Phones. With ADAC, you can automatically configure the switch to support and prioritize IP Phone traffic. Auto-detection by Link Layer Discovery Protocol (LLDP) (IEEE 802.1AB) allows the system to detect IP phones with MAC addresses outside the list of default MAC address ranges as long as they can be identified as an IP phone by LLDP, regardless of their MAC addresses.

Release 5.0 provides ADAC and 802.1AB interoperability, where an IP phone configured with Avaya automatic QoS can update phone 802.1q priority and DSCP values based on Network Policy 802.1AB Type, Length, and Value (TLV) elements sent by the switch on an ADAC telephony port. The LLDP compliant IP phone then uses the received Differentiated Services Code Point (DSCP) when sending voice traffic. Avaya Automatic QoS recognizes and prioritizes the traffic accordingly.

ADAC and 802.1AB interoperability is automatically enabled when Avaya automatic QoS, ADAC, and LLDP Network Policy TLV are enabled. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

802.1AB Customization features

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 in Release 5.0 by the additional customization makes LLDP suitable for deployments where a variety of vendor equipment or deployment methods exist. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

802.1AB Integration features

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 Type, Length, and Value (TLV) elements, 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. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

802.1AB LLDP new default parameters

Beginning with Release 5.0, you can improve Voice and Video over IP function because some of the LLDP parameters are enabled by default. Now you can connect LLDP enabled IP handsets to the switch and start deployment without additional configuration. The following LLDP parameters are enabled by default:

- lldp config-notification
- lldp status txAndRx config-notification
- lldp tx-tlv local-mgmt-addr | port-desc | sys-desc | sys-name
- lldp tx-tlv dot3 mdi-power-support
- lldp tx-tlv med extendedPSE | inventory | location | med-capabilities | network-policy

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

802.1AB (LLDP) Standards Based Auto Topology

You can enable the Optivity* Autotopology* protocol on the Ethernet Routing Switch 3500 Series with ACLI. For more information about Autotopology, go to the Avaya support site: http://support.avaya.com/css/appmanager/public/support (The product family for Optivity and Autotopology is Data and Internet.)

Autotopology is enabled by default.

802.1AB Location TLV

Release 5.0 provides support for optional organizationally-specific Type, Length, and Value (TLV) elements for use by Media Endpoint Devices (MED) and MED network connectivity devices. Location Identification TLVs allow network connectivity devices to advertise the appropriate location identifier information for an endpoint in use in the context of location-based applications. The Location Identification Discovery extension enables the advertisement of location identifier information to Communication Endpoint Devices (Class III), based on the configuration of the Network Connectivity Device to which it is connected. This is expected to be related to wiremap or similar network topology data, such that the configuration of the Network Connectivity Device can uniquely identify the physical location of the connected MED Endpoint, and hence the correct location identifier information for it to use. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

802.1AB MED

This feature enables additional VoIP plug and play capabilities by supporting the advertisement of IP Phone capabilities that specify VLAN and QoS with the 802.1AB Media Endpoint Discovery (MED) function. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

802.1p traffic class support / remarking

The Avaya Ethernet Routing Switch 3500 Series has four internal hardware CoS queues associated with each port for transmission of frames. The switch enables 802.1p Traffic Class by mapping the eight 802.1p priority levels into these four internal hardware CoS queues. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Quality of Service*, NN47203–503.

802.1Q tagging

The Ethernet Routing Switch 3500 Series allows tagging by port on all ports. Tagging status applies on all ports of a Multi-Link trunk (a port member in a Multi-Link trunk cannot be configured independently of the other members in the same Multi-Link trunk). You can configure untagged frame dropping by port.

The Ethernet Routing Switch 3500 Series supports the Independent VLAN Learning (IVL) model. IVL allows duplicate MAC addresses to be present in different sets, but not in the same set or VLAN. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2,* NN47203–500.

802.1w&s — rapid and multiple spanning trees

The current Spanning Tree implementation in Ethernet Routing Switch 3500 Series is based on IEEE 802.1d, which is slow to respond to a topology change in the network (such as a dysfunctional link in a network). The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. In certain configurations the RSTP recovery time is less than 1 second. It also maintains a backward compatibility with the IEEE 802.1d by allowing a port to be configured in STP (Spanning Tree Protocol) compatible mode. A port operating in STP compatible mode transmits and receives only STP BPDUs and drops any RSTP BPDUs.

RSTP also reduces the amount of flooding in the network by enhancing the way Topology Change Notification (TCN) packet is generated.

With Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), you can configured multiple instances of RSTP on the same switch. Each RSTP instance can include one or more VLANs. The operation of the MSTP is similar to the current Avaya proprietary MSTP. For more information on RSTP and MSTP, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — Layer 2*, NN47203–500.

802.1X EAP (SHSA, MHMA, MHSA, Guest VLAN, Non-EAP & RADIUS MAC)

The Avaya Ethernet Routing Switch 3500 Series provides security on the basis of Extensible Authentication Protocol over LAN (EAPOL), and it uses the EAP as it is defined in the IEEE 802.1X, so that you can set up a network access control over LANs. With EAP, you can authenticate user information through a connection between a client and the switch by using an authentication service such as RADIUS. This security feature works with the RADIUS-based server to provide the advantages of remote authentication to internal LAN clients. The ERS 3500 Series supports Basic EAP Authentication to configure Guest VLAN access. To allow multiple hosts and non-EAPOL clients on a port, the ERS 3500 Series supports some advanced EAPOL-supported operating modes such as : Multiple Host with Multiple Authentication (MHMA), Non-EAP IP phone authentication, Multiple Host with Single Authentication (MHSA), and Single Host with Single Authentication (SHSA). For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security,* NN47203–504.

802.1X Enhancement: Dynamic VLAN assignment for NEAP & MHMA

The Avaya Ethernet Routing Switch 3500 Series supports Multiple Host with Multiple Authentication (MHMA). This feature allows a finite number of EAP users or devices with unique MAC addresses on the port. MHMA support is on a per-port basis for an EAP-enabled port.

Dynamic RADIUS VLAN assignment is supported for only the first successfully authenticated EAP client that changes the current switch Port VLAN ID. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security,* NN47203–504.

802.1X Enhancement: Unicast request, Non-EAP IP Phone support

With unicast EAP requests in Multiple Host with Multiple Authentication (MHMA) enabled, the switch does not periodically query the connected MAC addresses to a port with EAP Request Identity packets. The clients must be able to initiate the EAP authentication sessions (send EAP Start packets to the switch) themselves. Not all EAP supplicants can support this operating mode.

Multicast mode is selected by default for all ports on the switch. You must set the EAP packet mode to unicast in both global and interface modes for switch ports to enable this feature. Any other combination (for example, multicast in global, unicast in interface mode) selects the multicast operating mode.

Non-EAP (NEAP) IP Phone authentication can be used for IP Phones that cannot authenticate with EAP. On an EAP capable IP Phone, EAP must be disabled to use non-EAP IP Phone authentication. DHCP must be enabled on the phone, because the switch examines the phone signature in the DHCP Discover packet sent by the phone.

For more information on Unicast requests and Non-EAP IP Phone support, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

802.1X NEAP accounting

EAP accounting provides RADIUS accounting for EAP-authenticated clients in the network. The RADIUS accounting protocol is defined in RFC 2866. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

802.1X NEAP and Guest VLAN on same port

With this enhancement you can now configure the 802.1X, Non-EAP, and Guest VLAN functions on the same port simultaneously for a more universal port configuration. You do not have to configure a port to support Guest VLANs or Non-EAP or 802.1X; one port can support all three functions. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

802.1X NEAP fail-open VLAN

The 802.1X NEAP with fail open VLAN feature provides network connectivity when the switch cannot connect to the RADIUS server. If connectivity to the RADIUS servers is lost, all authenticated devices most into the configured fail open VLAN. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

802.1X NEAP last assigned VLAN

The 802.1X NEAP Last Assigned RADIUS VLAN feature allows an EAP or non-EAP client to use the most recent RADIUS assigned VLAN. The Last Assigned RADIUS VLAN determines the VLAN membership and PVID values for the port. For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — Security*, NN47203–504.

802.1X NEAP re-authentication timer

You can use 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. 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. For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — Security*, NN47203–504.

802.1X NEAP with VLAN names

When you use the 802.1X or non-EAP with VLAN names functionality, the switch can match RADIUS assigned VLANs based on either the VLAN number or the VLAN name. Because the 802.1X or non-EAP with VLAN names mode is always enabled, you do not have to configure this feature. The VLAN number or name can be used to configure VLAN membership of EAP or non-EAP clients. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

802.1X RFC 2866/2869 RADIUS interim accounting updates

RADIUS interim accounting updates support permits the RADIUS server to make policy decisions based on real-time network attributes transmitted by the Network Access Server (NAS).

An example of how RADIUS Interim Accounting Updates support enhances network security is the Threat Protection System (TPS) alerting the Dynamic Authorization Client (RADIUS server) about abnormal traffic patterns from a specific IP address on the network. The RADIUS server can correlate IP address to MAC address information in the internal session database, locate the device access point on the network, and issue a Change-Of-Authorization or Disconnect message to NAS.

Support for RADIUS interim accounting updates is not enabled by default. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

802.1X RFC 3576 RADIUS auth extensions - CoA

With 802.1X dynamic authorization extension (RFC 3576), you can enable a third party device to dynamically change VLANs on switches or close user sessions.

The 802.1X dynamic authorization extension process includes the following device:

- RADIUS server — sends disconnect and Change of Authorization (CoA) requests to the AAS. A CoA command modifies user session authorization attributes and a disconnect command ends a user session.

For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — Security*, NN47203–504.

802.3ad- Link Aggregation Control Protocol (LACP)

You can create and manage a trunk group with Link Aggregation (LA). You can control and configure a trunk group automatically using the Link Aggregation Control Protocol (LACP)

The LACP, defined by IEEE802.3ad standard, allows the switch to learn the presence and capabilities of a remote switch by exchanging information with the remote switch before a trunk group is formed. Either switch can accept or reject the aggregation request with the far end on a per port basis. A link that can not join a trunk group operates as an individual link. 802.3ad provides an industry standard method for bundling multiple links together to form a single trunk between two networking devices. Trunks that confirm to the 802.3ad standard are Link Aggregation Groups (LAGs). For more information on LACP, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

802.3af (Power over Ethernet —PoE) and 802.3at (PoE+)

The Ethernet Routing Switch 3526T-PWR+, 3510GT-PWR+, and 3524GT-PWR+ support IEEE802.3af-compliant power and IEEE802.3at-compliant power on all front-panel RJ-45 ports contained within the orange line on the PWR+ models. The switches provide power discovery, power management, and statistics on power use on a per port and per switch basis. You can use the Ethernet Routing Switch 3500 Series to provide power to network appliances, such as IP telephones, Wireless LAN Access Points, and video devices. IEEE802.3af (PoE) standard defines power support of up to 15.4W (300mA at source) while IEEE802.3at (PoE+) standard defines power support of up to ~32W (600mA at source) per port.

The Ethernet Routing Switch 3510GT-PWR+, 3526T-PWR+/3524GT-PWR+ provide Power over Ethernet (PoE/PoE+) on 8 and 24 ports respectively. The ERS 3526T-PWR+ and ERS 3524GT-PWR+ switches provide a maximum of 370 Watts of power budget across 24 PoE ports on each switch. Adequate power is available to support, on average, 15.4 Watts for each port on the 3524GT-PWR+ and 3526T–PWR+ models.

The ERS 3510GT-PWR+ can operate in one of two different power “modes”. Low Power Budget mode provides a maximum PoE budget of up to 60W across 8 ports (fanless mode), while High Power Budget mode provides a maximum of 170 Watts of power across 8 ports (fan mode). This provides average concurrent power of 7.5W per port in Lower Power Budget mode or 21.25W per port in High Power Budget mode.

The Ethernet Routing Switch 3510GT-PWR+, 3524GT-PWR+, and 3526T-PWR+ supply data terminal equipment (DTE) power only on signal pair pins.

By default, power is allocated based on real time measurements. If the total Ethernet power budget for the switch is exceeded, the switch sheds load by shutting down power to ports.

Configure Power over Ethernet (PoE) parameters on the PoE ports with ACLI or Enterprise Device Manager (EDM). For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

802.3x (Flow Control — Gig ports only)

The high speed flow control feature lets you control traffic and avoid congestion on the gigabit full-duplex link. If the receive port buffer becomes full, the Ethernet Routing Switch 3500 Series issues a flow-control signal to the device at the other end of the link to suspend transmission. When the receive buffer is no longer full, the switch issues a signal to resume the transmission. You can choose Symmetric or Asymmetric flow control mode. High speed flow control cannot be configured unless you set Autonegotiation to Disabled on the port and the speed/duplex is at 1000/full. For more information on configuring flow control, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

ACLI

Avaya Command Line Interface (ACLI) is a text-based interface used for switch configuration and management. A common command line interface (CLI), ACLI follows the industry standard for device management across Avaya products.

ACLI command modes occur in order of increasing privileges, each based on user logon permission level. Logon password determines logon permission level.

You can access ACLI directly through a console connection, remotely through a dial-up modem connection, or in-band through a Telnet session. For more information on ACLI command modes and access procedures, see *Avaya Ethernet Routing Switch 3500 Series — Fundamentals*, NN47203–102.

Advanced QoS

Advanced QoS supports improved traffic control and offers Layer 2, 3, and 4 traffic classification. When you use Advanced QoS capability you can identify traffic flows using filters and you can apply user-defined actions to the traffic flows. Actions that you can apply to traffic flows include:

- Drop
- Forward
- Mark or Re-mark — the DiffServ Code Point (DSCP)
- Meter/Police — ingress rate limiting
- Shape — egress flow control

For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — Quality of Service* , NN47203–503.

ASCII Config Generator (ACG)

The primary goal of the ASCII Configurator Generator (ACG) is to provide the users of the Ethernet Routing Switch 3500 Series with a tool that lets them easily modify the configuration of a particular switch.

ACG generates an ASCII configuration file which reproduces the behaviour of the current binary configuration file. The user can also rely on this function to maintain backup configurations, as well as use it as a reliable method for debugging the current configuration of a switch.

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

ASCII file configuration

The Ethernet Routing Switch 3500 Series can download an editable ASCII configuration file from the TFTP server. You can load the ASCII configuration file automatically at start time or on demand using console menus or ACLI. After the editable ASCII configuration file is downloaded, the configuration file automatically configures the switch according to the Avaya Command Line Interface (ACLI) commands in the file. The maximum size for an ASCII configuration file is 100 KBs; larger configuration files must be split into multiple files. For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Auto Detection And Configuration (ADAC) with 802.1AB interaction

Auto-Detect Auto-Configuration (ADAC) provides a plug and play mechanism for automatically detecting an IP Phone based on MAC address using the switch's internal MAC list, or using the user defined MAC list for detection, and then configuring VLAN membership and QoS for the switch port. 802.1AB (LLDP) interaction provides an alternate method for detecting an IP Phone using LLDP regardless of the IP Phone MAC address.

Recent enhancements to ADAC added increased flexibility in deployments that use ADAC as follows:

- Support for up to eight ADAC uplinks and eight Call Server links (individual ports or any combination of MLT and LAG) for each switch .
- Ability to change the non-ADAC VLANs on a port without disabling ADAC.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–501.

Auto Save configuration enhancements

By default, every 60 seconds the Ethernet Routing Switch checks whether a configuration change has occurred, or if a log message is written to nonvolatile storage. If one of these two events has occurred, the system automatically saves its configuration and the nonvolatile log to flash memory. Also, the system automatically saves the configuration file if a system reset command is invoked by the user.

For more information on enabling and disabling the Auto Save feature, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Avaya Automatic QoS

When you enable Avaya Automatic QoS (AAQ), the switch recognizes Avaya application traffic and prioritizes the traffic through the switch. Avaya Automatic QoS is enabled or disabled globally and the feature offers a simplified and resource-efficient mechanism to prioritize Avaya application traffic within your network.

After you enable AAQ, automatic QoS is applied end-to-end, from the application traffic to the Avaya or third party data infrastructure, and non-Avaya application traffic is unaffected. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Quality of Service*, NN47203–503.

BootP/DHCP Relay

Dynamic Host Configuration Protocol (DHCP) is a mechanism to assign network IP addresses on a dynamic basis to clients who request an address. DHCP is an extension of the Bootstrap protocol (BootP). BootP/DHCP Clients (workstations) generally use User Datagram Protocol (UDP) broadcasts to determine their IP addresses and configuration information. If such a host is on a VLAN that does not include a DHCP server, the UDP broadcasts are by default not forwarded to servers located on different VLANs.

The Avaya Ethernet Routing Switch 3500 Series can resolve this issue using DHCP relay, which forwards the DHCP broadcasts to the IP address of the DHCP server. Network managers prefer to configure a small number of DHCP servers in central locations to lower administrative overhead. Routers must support DHCP relay so that hosts can access configuration information from servers several router hops away.

With DHCP relay enabled, the switch can relay client requests to DHCP servers on different Layer 3 VLANs or in remote networks. It also relays server replies back to the clients. For more information on BootP/DHCP relay, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — IP Routing/Multicast*, NN47203–502.

BootP or Default IP

The Ethernet Routing Switch 3500 Series operates in the BootP or Default IP mode (the default mode) as follows:

- After the switch is reset or power cycled, if the switch has a configured IP address other than 0.0.0.0 or the default IP address then the switch uses the configure IP address.
- If the configured IP address is 0.0.0.0 or the default address (192.168.1.1/24) then the switch attempts BootP for 1 minute.
- If BootP succeeds then the switch uses the IP information provided.
- If BootP fails and the configured IP address is the default then the switch uses the default IP address (192.168.1.1/24).
- If BootP fails and the configured IP address is 0.0.0.0 then the switch retains this address.

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

BPDU Filtering

The Spanning Tree Protocol (STP) detects and eliminates logical loops in a bridged or switched network. Any bridge that participates in the spanning tree exchanges information with other bridges using configuration messages known as Bridge Protocol Data Units (BPDU). Based on the BPDU information exchange, the bridge with the lowest bridge ID becomes the root. This process is called the root selection process.

The BPDU-Filtering features allows the network administrator to achieve the following:

- Block an unwanted root selection process when an edge device, such as a laptop running Linux and enabled with STP, is added to the network. This prevents unknown devices from influencing an existing spanning tree topology.
- Block the flooding of BPDUs from an unknown device.

Note:

The STP PBDU-Filtering feature is not supported on Multi-Link Trunk (MLT) ports.

For more information on BPDU filtering, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

CANA

Custom Autonegotiation Advertisements (CANA) lets you customize the capabilities that you advertise. For example, if a port is capable of 10/100/1000 full duplex operation, the port can be configured to only advertise 10 half-duplex capabilities.

CANA lets you control the capabilities that are advertised by the Ethernet switches as part of the autonegotiation process. In the current software release, autonegotiation can either be enabled or disabled.

When autonegotiation is disabled, the hardware is configured for a single (Fixed) speed and duplex value. When autonegotiation is enabled, the advertisement made by the product is a constant value based upon all speed and duplex modes supported by the hardware.

When autonegotiating, the switch selects the highest common operating mode supported between the switch and its link partner.

Important:

The CANA feature is available only for built-in 10/100 Ethernet ports and combo ports (not available for rear ports).

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

CLI Quick Start script

You can use the **`install`** command to configure the in-band IP Address and netmask, default gateway, read-only and read-write community strings, quick start VLAN, and IPv6 in-band address and IPv6 default gateway with ACLI.

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

Configurable SNMP trap port (only SNMP v1 & v2)

You can use Enterprise Device Manager (EDM) to enable or disable traps received by the SNMP trap receiver. You can also create a host notification profile to specify which traps a host receives. This is available in EDM and ACLI. For more information , see *Avaya Ethernet Routing Switch 3500 Series-Configuration — Security*, NN47203–504.

Configure Asset ID

You can configure the Asset ID with ACLI commands or EDM. An Asset ID provides inventory information for the switch. For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

COS/DSCP — allows mapping the DSCP value (carried by IP frames) to 802.1p priority value

The Quality of Service (QoS) Class of Service (COS) directs which group of packets receives the best network throughput. The level of service for each packet is determined by the configurable DSCP. The available levels of QoS classes are Network, Premium, Platinum, Gold, Silver, Bronze, and Standard. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Quality of Service*, NN47203–503.

CPU and Memory Utilization

The CPU and Memory Utilization feature provides data for CPU and memory utilization. You can view CPU utilization information for the past 10 seconds (sd), 1 minute (min), 1 hour (hr), 24 hr, or since system startup. The switch displays CPU utilization as a percentage. With CPU utilization information you can see how the CPU was used during a specific time interval.

The memory utilization provides information about the percentage of the dynamic memory currently used by the system. The switch displays memory utilization in terms of the lowest percentage of dynamic memory available since system startup.

No configuration is required for this display-only feature. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

Cumulative system uptime

Enterprise Device Manager tracks a wide range of statistics for the switch and each port. The data tables in the statistics dialog boxes list the counters, or categories of statistics being gathered, for the selected object. One of the types of statistics that is available is a Cumulative Statistic which provides the total count since the statistics window was first opened. The elapsed time for the cumulative counter is displayed at the bottom of the graph window. For more information on this, and other statistics, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

DA Filtering

If MAC address-based security software detects a security violation, one of the optional switch settings is that the response can turn on destination address (DA) filtering. This switch setting is enabled or disabled using the **`mac-security`** command. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

DHCP Client

The Avaya Ethernet Routing Switch 3500 Series now supports Dynamic Host Configuration Protocol (DHCP) relay, which forwards DHCP broadcasts to the IP address of a remote DHCP server. Routers must support DHCP relay so that hosts can access configuration information from servers that are several router hops away. DHCP Client for switch provides an alternative method to assign an IPv4 address to the Management VLAN. For more information , see *Avaya Ethernet Routing Switch 3500 Series - Configuration — IP Routing/Multicast*, NN47203–502.

DHCP Snooping

Dynamic Host Configuration Protocol (DHCP) snooping provides security to the network by preventing DHCP spoofing. DHCP spoofing is the ability of an attacker to respond to DHCP requests with false IP information. DHCP snooping acts as a firewall between untrusted hosts and the DHCP servers, so that DHCP spoofing cannot occur. DHCP snooping classifies ports as untrusted or trusted.

Untrusted ports are configured to receive messages from outside the network or firewall. Only DHCP requests are allowed.

Trusted ports are configured to receive messages only from within the network, such as switch-to-switch and DHCP server ports. All types of DHCP messages are allowed.

DHCP snooping is configured on a VLAN-to-VLAN basis. For more information on DHCP Snooping, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

Distributed LAG (802.3ad) LACP, up to six trunks with four links per trunk

The Avaya Ethernet Routing Switch 3500 Series supports distributed link aggregation for up to six trunks with four active ports per group. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–501.

Domain Name Service (DNS) capability

You can use the Domain Name Server (DNS) client to ping or Telnet to a host server or to a host by name. To use this feature, you must configure at least one DNS. You can also configure a default domain name. If you configure a default domain name, that name is appended to host names that do not contain a dot. The default domain name and addresses are saved in NVRAM. The host names for ping and Telnet cannot be longer than 63 alphanumeric characters, and the default DNS domain name cannot be longer than 255 characters.

For more information on enabling and disabling the Auto Save feature, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Downloading agent & diags without reset

You can update switch software with an active image (primary) or non-active (secondary) image using ACLI commands or EDM. The non-active image is also known as the Next Boot Image. The Next Boot image is an agent image that is stored in the flash memory to be used for the next boot.

When an agent image is downloaded to the switch, the unit resets and boots up with the newly downloaded image regardless of the value of the Next Boot image indicator. If an agent image is downloaded to the switch without a reset of the unit, the newly downloaded image becomes the Next Boot image.

The parameter diag can be used with the **`download`** command to specify the name of the diagnostic image to be downloaded from the TFTP serer.

For more information on downloading agent and diagnostics, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started* , NN47203–301.

Dual Syslog servers

You can use the Dual Syslog Server support feature to configure a second syslog server to run in tandem with the first. If you configure two Syslog server IP addresses, the switch sends Syslog messages to both servers simultaneously to ensure that Syslog messages are recorded, even if one of the servers becomes unavailable. For more information, see *Avaya Ethernet Routing Switch - Configuration — System Monitoring*, NN47203–501.

Dynamic ARP Inspection

Dynamic Address Resolution Protocol (Dynamic ARP) inspection is a security feature that validates ARP packets in the network.

Without Dynamic ARP inspection, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Dynamic ARP inspection prevents this type of man-in-the-middle attack. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

Extended IP Manager (IPv4 & IPv6)

With IP Manager, you can limit access to the management features of the Avaya Ethernet Routing Switch 3500 Series by defining the IP addresses that are allowed access to the switch.

With the IP Manager, you can do the following:

- define a maximum of 50 IPv4 and 50 IPv6 addresses, and masks that are allowed to access the switch. No other source IP addresses have management access to the switches.
- enable or disable access to Telnet, SNMP, SSH, and Web-based management system.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

Factory-default command

The **`restore factory-default`** command resets the switch to its default configuration. For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started* , NN47203–301.

HTTP port change

With this feature, you can define the UDP or TCP port number used for HTTP connections to the switch.

This feature provides enhanced security and network access. Port number 80 is the default port for communication between the Web client and the server. With this feature, you can modify the HTTP port while the switch is running. The HTTP port value is saved in NVRAM, and also is saved across reboots of the switch. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

HTTPS/SSL secure web management

The management interfaces of the Avaya Ethernet Routing Switch 3500 Series (ACLI/SNMP) can configure the Web server to operate in a secure or non-secure mode. The Secure Socket Layer (SSL) Management Library interacts with the Web server to this effect.

In the secure mode, the Web server listens on TCP port 443 and responds only to HTTPS client browser requests. All existing non-secure connections with the browser are closed down.

In the non-secure mode, the Web server listens on TCP port 80, by default, and responds only to HTTP client browser requests. All existing secure connections with the browser are closed down. The TCP port can be designated as any number from 1024 to 65535. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

HTTP web-based management

Enterprise Device Manager (EDM) is an embedded element management and configuration application for Avaya Ethernet Routing Switch 3500 Series switches. EDM uses a Web-based graphical user interface for the convenience of full integration onto the switch. You can use EDM element management to set up, stage, and configure switches and monitor device statistics. To use EDM you require only an internet browser.

EDM is available as:

- an embedded, on-box version accessed by a Web browser and available by default on every switch
- an off-box version available as a free, downloadable software plug-in installed on Configuration and Orchestration Manager (COM), purchased separately

Procedures using EDM are provided throughout the *Avaya Ethernet Routing Switch 3500 Series* suite of documents. For more information on EDM fundamentals, see *Avaya Ethernet Routing Switch 3500 Series — Fundamentals*, NN47203–102.

Identify Units (Blink LEDs)

With the **`blink-leds`** command, you can set the LEDs on the display panel of each ERS 3500 Switch to blink to identify a particular unit. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

IGMP Multicast no flood command enhancements

On the Ethernet Routing Switch 3500 Series you can enable the unknown multicast filtering feature so that the unknown multicast packets are not flooded to the VLAN. With this feature enabled, the switch forwards all unknown multicast traffic to IGMP static mrouter ports only. The traffic is not forwarded to dynamically discovered mrouter ports. If you require unknown multicast traffic to be forwarded to certain ports (for example, to forward Layer 3 multicast routing traffic), set the ports as static mrouter ports. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — IP Routing/Multicast*, NN47203–502.

IGMPv1/v2 snooping / proxy

To prune ports that are not group members from receiving the group data, the Avaya Ethernet Routing Switch 3500 Series supports Internet Group Membership Protocol (IGMP) snoop for IGMPv1 and IGMP v2. With IGMP snoop enabled on a VLAN, the switch forwards the multicast group data to only those ports that are members of the group. When using IGMP snoop, VLANs can provide the same benefit as IP Multicast routers, but in the local area.

With IGMP snoop enabled, the switch can receive multiple reports for the same multicast group. Rather than forward each report upstream, the Ethernet Switch 3500 Series can consolidate these multiple reports by using the IGMP proxy feature. With IGMP proxy enabled, if the switch receives multiple reports for the same multicast group, it does not transmit each report to the upstream multicast router. Instead, the switch forwards the first report to the querier and suppresses the rest. If new information emerges that another multicast group is added or that a query is received because the last report is transmitted upstream, the report is then forwarded to the multicast router ports. To enable IGMP Proxy, you must first activate IGMP snooping. For more information, see *Avaya Ethernet Routing Switch 3500 Series– Configuration — IP Routing/Multicast*, NN47203–502.

IGMPv3 Snooping/proxy

With IGMPv3 proxy enabled, if the switch receives multiple reports for the same multicast group, it does not transmit each report to the upstream multicast router. Instead, the switch forwards the first report to the querier and suppresses the rest. If new information emerges, for example, if the switch adds another multicast group or receives a query since the last report was transmitted upstream, then the switch forwards a new report to the multicast router ports.

In IGMPv3 snooping mode, the switch recognizes IGMPv3 reports and queries and can:

- recognize whether a source list is populated or blank
- identify the specific sources to filter for every multicast group a client joins
- understand and process all IGMPv3 query types, INCLUDE and EXCLUDE IGMPv3 report types

The following are supported:

- source filtering based on ALLOW and BLOCK, IGMPv3 report types

For more information on IGMPv3 snooping/proxy, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — IP Routing/Multicast*, NN47203–502.

IP Local and Non-Local Static routing

In this release, the Avaya Ethernet Routing Switch 3500 Series supports local routes and static routes. With local routing, the switch automatically creates routes to each of the local Layer 3 VLAN interfaces. With static routing, you must manually enter the routes to the destination IP addresses. With routing globally enabled, if you assign an IP address to a VLAN, IP routing is enabled for that VLAN. In addition, for each IP address assigned to a VLAN interface, the Ethernet Routing Switch adds a directly connected or local route to its routing table based on the IP address/mask assigned. For a route to become active, the corresponding next-hop IP address must be reachable through a directly connected subnet. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — IP Routing/Multicast*, NN47203–502.

IP Source Guard

IP Source Guard provides security to the network by filtering clients with invalid IP addresses. It is a Layer 2 feature for each port that works closely with information in the Dynamic Host Control Protocol (DHCP) snooping Binding Table. When IP Source Guard is enabled on an untrusted port with DHCP snooping enabled, an IP filter entry is created or deleted for that port automatically, based on IP information stored in the corresponding DHCP snooping Binding Table entry. When a connecting client receives a valid IP address from the DHCP server, a filter is installed on the port to allow traffic only from the assigned IP address. A maximum of 10 IP addresses are allowed on each IP Source Guard-enabled port. When this number is reached, no additional filters are set up and traffic is dropped. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

IPv6 Management

In Release 5.0, the Ethernet Routing Switch 3500 Series does not support stateless or stateful address configuration. The device does not try to obtain IPv6 parameters from a router and it does not query an IPv6 DHCP server, if it does not have an IPv6 address configured. The IPv6 global address of the ERS 3500 series switch must be entered manually. The link-local IPv6 address is generated automatically based on the MAC address of the device, once the IPv6 interface is attached to the management VLAN.

IPv6 VLANs (protocol based)

IPv6 recognition through the configuration of protocol-based VLANs for segmenting IPv6 traffic is supported. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

Local console via serial interface

The Console port is an RJ-45 port. You can use this connector to connect a management station, console, or terminal to the Ethernet Routing Switch 3500 Series by using either an integrated console cable with DB-9 female connector at one end and RJ-45 for switch console port or an RJ-45 to DB-9 adaptor used with straight Cat 5E cable. For instructions on console port settings, see *Avaya Ethernet Routing Switch 3500 Series — Quick Install Guide*, NN47203–300.

Local password protection

You can set a local user name and password to restrict access to the Ethernet Routing Switch 3500 Series. The user name and password can provide read/write access or read-only access to the switch. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

MAC address based security with autolearn (BaySecure)

Use the MAC address-based security to set up network access control based on source MAC addresses of authorized stations. You can perform the following activities:

- create a list of up to 448 MAC addresses and specify which addresses are authorized to connect to your switch
- specify which switch port each MAC address can access
- specify optional switch actions if the software detects a security violation

The MAC address-based security feature is based on Avaya BaySecure LAN Access for Ethernet, a real-time security system that safeguards Ethernet networks from unauthorized surveillance and intrusion.

The MAC address-based security autolearning feature provides the ability to add allowed MAC addresses to the MAC Security Address Table automatically without user intervention. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

MAC flush

Use the MAC flush feature to clear MAC Address entries directly from the MAC Address Table (or Forwarding Data Base). MAC Flush provides the following options to flush out MAC Address entries:

- clear a single MAC Address
- clear all addresses in the MAC address table
- clear all MAC addresses from a port (or list of ports)
- clear all MAC addresses from a trunk (MLT or LAG)
- clear all MAC addresses from a particular VLAN

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

MLT enable/disable whole trunk

Use the Multi-Link Trunk (MLT) enabled or disable whole trunk feature to enable or disable trunk loop prevention for MLT. The feature is disabled by default. If you enable the feature, the state of the port changes to reflect the state of the MLT bundle irrespective of the previous status. If you disable the MLT then all links that are part of the MLT group are disabled, with the exception of the Destination Lookup Failure (DLF) link. For network configuration, Avaya recommends that you enable the MLT whole trunk feature. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

Multi-Link Trunking (MLT)

The Multi-Link Trunking (MLT) feature is a point to point link aggregation function that allows you to group multiple switch ports together, when forming a link to another switch or server. This provides additional link redundancy and increases the aggregate throughput of the interconnection between the two devices.

The Ethernet Routing Switch 3500 Series can be configured with up to six (6) Multi-Link Trunk groups, of up to four (4) links within each group. Multi-Link Trunking software detects broken trunk links and redirects traffic from the broken trunk link(s) to other trunk members within that trunk. For more information on MLT, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

No Banner & CTRL-Y Skip

You can customize the banner than appears when you connect to the Ethernet Routing Switch 3500 Series. You can customize the text that reads `AVAYA.` However you cannot customize the second line that reads `Enter [Ctrl]+y` to begin. The **`no banner`** command lets you clear all lines of a previously stored custom banner.

If you choose not to display the banner, the system enters the command mode through the default command interface. You do not have to press the `[Ctrl]+y` keys. For more information on the Banner Control feature, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Ping enhancement

The **`ping`** command tests the network connection to another network device. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device. The local IP address must be set before issuing the command. You can use the ping command to specify additional ping parameters, including the number of ICMP packets to be sent, the packet size, the interval between packets, and the timeout. You can also set the ping to continuous, or you can set a debug flag to obtain extra debug information.

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

Port mirroring (1–1)

With the Port Mirroring feature (also known as conversation steering), you can allocate a single switch port (monitor port) as a traffic monitor for another switch port (mirror port). All incoming traffic on the mirrored port is copied to the monitor port. This operation excludes traffic forwarded by the switch. This feature is helpful in network troubleshooting. For more information on port mirroring, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

Port Naming

You can name a port with ACLI. The **`name`** command lets you name ports or change the port name. The **`no name`** and **`default name`** commands clear the port names and reset the field to an empty string. For more information on port naming, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Proxy ARP

Proxy Address Resolution Protocol (ARP) allows the Ethernet Routing Switch 3500 Series to respond to an ARP request from a locally attached host that is intended for a remote destination. It does so by sending an ARP response back to the local host with the MAC address of the switch interface that is connected to the host subnet. The reply is generated only if the switch has an active route to the destination network.

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

RADIUS-based security

Remote Access Dial-In User Services (RADIUS) is a distributed client server system that helps secure networks against unauthorized access, allowing a number of communication servers and clients to authenticate user identities through a central database. The database within the RADIUS server stores information about clients, users, passwords, and access privileges; these are protected by a shared secret.

RADIUS authentication is a fully open and standard protocol defined by RFC 2865. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

RADIUS EAP / NEAP to different servers

You can separate EAP and non-EAP 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 non-EAP requests. NOTE: the non-EAP RADIUS server is not used for ports in SHSA or MHSA mode since neither mode supports non-EAP.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

RADIUS password fallback

You can configure RADIUS password fallback as an option when you use RADIUS authentication for logon and password. When RADIUS password fallback is enabled and the RADIUS server is unavailable or unreachable, you can use the local switch password to log on to the switch. When RADIUS password is disabled, you must specify the RADIUS user name and password from the NetLogin screen. Unless the RADIUS server is configured and reachable, you cannot log on to the switch to authenticate the logon and password. The RADIUS password fallback feature is disabled by default. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

RADIUS Server reachability

You can use RADIUS server reachability to configure the switch to use ICMP packets or dummy RADIUS requests to determine the reachability of the RADIUS server. The switch regularly performs the reachability test to determine if the switch should fail over to the secondary RADIUS server or to activate the fail open VLAN, if that feature is configured on the switch. If you implement internal firewalls which limit the flow if ICMP reachability messages from the switch to the RADIUS server, you can configure the switch to use dummy RADIUS requests. If the switch is configured to use dummy RADIUS requests, the switch generates a regular dummy RADIUS request with the username 'avaya'. It is recommended that you set up a dummy account with the user name avaya on the RADIUS server to avoid the generation of error messages indicating invalid user logins, if RADIUS server reachability is enabled. By default, the switch uses ICMP packets to determine the reachability of the RADIUS server.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

Rate Limiting

The Rate Limiting feature lets you configure the threshold limits for broadcast and multicast packets ingressing on a port for a given time interval. The Ethernet Routing Switch 3500 Series drops packets received above the threshold value if the traffic ingressing on the port exceeds the threshold. The hardware restrictions on this platform do not allow you to determine if the traffic from a port is the cause of excess broadcast or multicast traffic. Consequently you cannot perform port specific actions such as disabling a port. You can generate a trap to detect the excess traffic or you can configure the switch to store a message in the system log when the traffic on the port exceeds the threshold value. This message in the system log conveys that some traffic to the switch is dropped.

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

Remote logging

As part of configuring system logging, you can specify remote logging parameters. This involves configuring a remote syslog address, enabling remote logging and configuring the remote logging level.

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

RMON (RFC1757): per port Statistics, History, Alarm and Events

Remote Monitoring (RMON) MIB is an interface between the RMON agent on an Ethernet Routing Switch 3500 Series switch and an RMON management application, such as Enterprise Device Manager. The RMON agent defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular.

The RMON agent continuously collects statistics and proactive monitors switch performance. You can view this data through A\CLI and EDM.

RMON has three major functions:

- creating and displaying alarms for user-defined events
- gathering cumulative statistics for Ethernet interfaces
- tracking a history of statistics for Ethernet interfaces

For more information on RMON per port Statistics, History, Alarms and Events, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

Secure FTP (SFTP)

To provide secure file transfer functions, release 5.0 includes support for Secure FTP over a Secure Shell (SSH) session to the switch. Secure FTP on the ERS 3500 series only allows transfer of the binary configuration file.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

Show environmental

You can use this feature to display environmental information about the operation of the switch. The information includes power supply status, fan status, and switch system temperature. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

Show MAC address enhancement

You can view the contents of the MAC address forwarding database table, and filter the MAC Address table by port number. The MAC Address table can store up to 16000 addresses. For procedures to display MAC Address information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

Show Running Config enhancement

To display the current configuration of the switch, use the **`show running-config`** command. The entire configuration, including defaults and non-defaults can be displayed if you add the verbose variable. You can also display the configuration of an application for any of the following parameters with the module <value> variable: 802.1AB, adac, arp-inspection, banner, core, dhcp-relay, dhcp-snooping, eap, interface, ip, ip-source-guard, ipmgr, ipv6, l3, l3–protocols, lacp, logging, mac-security, mlt, poe, port-mirroring, qos, rate-limit, rmon, rtc, snmp, ssh ssl, stp, vlacp, vlan. For more information see, *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Show software status

The **`show boot`** ACLI command or the Boot Image EDM tab can display the currently loaded and operational software status for both agent and diagnostic images.

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

Shutdown, reload enhancement

The **`shutdown`** command provides a mechanism for safely shutting down a switch without interfering with device processes or corrupting the software image. After this command is issued, the configuration is saved, auto-save functionality is temporarily disabled, and configuration changes are not allowed until the switch restarts. If the shutdown is cancelled, auto-save functionality returns to the state in which it was previously functioning.

The **`reload`** command operates in a similar fashion to the **`shutdown`** command. However, the **`reload`** command is intended more to be used by system administrators using the command functionality to configure remote devices and reset them when the configuration is complete.

The **`reload`** command differs from the **`shutdown`** command in that the configuration is not explicitly saved after the command is issued. This means that any configuration changes must be explicitly saved before the switch reloads. The **`reload`** command does temporarily disable auto-save functionality until the reload occurs. Cancelling the reload returns auto-saved functionality to any previous setting. For more information on these commands, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Single 802.1d Spanning Tree Protocol (STP) on all ports

The Ethernet Routing Switch 3500 Series supports transparent bridging by implementing the IEEE 802.1d standard. This standard is known as the Spanning Tree Protocol (STP) and Spanning Tree Algorithm (STA) standards. STP runs on all ports to provide automatic network configuration of a loop-free topology. You can configure redundant links to provide network fault tolerance with STP. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2* , NN47203–500.

SNMP-based network management

The Avaya Ethernet Routing Switch 3500 Series supports Simple Network Management Protocol (SNMP) — SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2), and SNMP version 3 (SNMPv3). This protocol is traditionally used to monitor Unix systems, Windows systems, printers, modem racks, switches, routers, power supplies, Web servers, and databases. Any device that runs software that can retrieve SNMP information can be monitored.

You can also use SNMP to change the state of SNMP-devices. For example, you can use SNMP to shut down an interface on your device. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

SNMP MIB web page in EDM

You can use the EDM MIB Web page to view the response of the SNMP Get and Get-Next request for an Object Identifier (OID) or object name. With the SNMP walk, you can retrieve a subtree of the Management Information Base (MIB) that has the object as root by using Get-Next requests.

The MIB Web page does not support the following features:

- displaying SNMP SET requests
- displaying SNMP tables
- translating MIB enumerations (that is, displaying the name [interpretation] of number values of objects defined as enumerations in the MIB).

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

SNMP trap enhancements

With SNMP management, you can configure SNMP traps to automatically generate notifications globally, or on individual ports. These notifications can report conditions such as an unauthorized access attempt or changes in port operating status. All notifications are enabled on individual interfaces by default

The Avaya Ethernet Routing Switch 3500 Series supports both industry-standard SNMP traps, as well as private Avaya enterprise traps. SNMP trap notification-control provides a generic mechanism for the trap generation control that works with any trap type.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

SNMP Trap list web page in EDM

You can use Enterprise Device Manager (EDM) MIB Web page to query SNMP objects on the switch. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

SNMPv3 security

The Avaya Ethernet Routing Switch 3500 Series supports Simple Network Management Protocol (SNMP), SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2). This protocol is traditionally used to monitor Unix systems, Windows systems, printers, modem racks, switches, routers, power supplies, Web servers, and databases. Any device that runs software that can retrieve SNMP information can be monitored.

SNMP Version 3 (SNMPv3) is the current formal SNMP standard defined in RFCs 3410 through 3419, and in RFC 3584. It provides support for strong authentication and private communication between managed entities. SNMPv3 introduces industrial-grade user authentication and message security. This includes MD5– and SHA-based user authentication and message integrity verification, as well as AES, DES, and 3DES-based privacy encryption. You can configure SNMPv3 using the Enterprise Device Manager or ACLI. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

SNTP & SNTP timezone enhancement

The Simple Network Time Protocol (SNTP) feature synchronizes the Universal Coordinated Time (UTC) to an accuracy within 1 second. This feature adheres to the IEEE RFC 2030 (MIB is the s5agent). With this feature, the system can obtain the time from any RFC 2030–compliant NTP/SNTP server.

SNTP uses UTC for all time synchronizations so it is not affected by different time zones. There are a number of commands that are added in Release 5.0 to allow the switch to report the correct time for your local time zone and daylight savings time. The local time zone and daylight savings time can also be configured using EDM. For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Software Exception Log

This feature allows an administrator to see the software exceptions generated in the switching system. The software exception log provides a method for capturing software faults in the SYSLOG application as critical customer messages. The CLI allows you to display and clear the last software exceptions generated in the system. For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — System Monitoring,* NN47203–501.

Spanning Tree 802.1d compliance mode

The Ethernet Routing Switch 3500 Series supports the Spanning Tree Protocol (STP) as defined in IEEE 802.1d. STP 802.1d compliance mode ensures that STP conforms to the IEEE 802.1d standard.

IEEE 802.1d indicates that when a port link fails, the STP state of the port should stay in Forwarding mode. When STP 802.1d compliance mode is disabled, the switch is provided a fast recovery mechanism for a port that frequently changes state from up to down. This fast recovery mechanism does not comply with IEEE 802.1d standard, so when STP 802.1d compliance mode is enabled, the fast recovery mechanism is no longer available and the passing from blocking to forwarding state is done through listening and learning states. When a port link fails, the STP state of the port is Forwarding if STP 802.1d compliance mode is disabled and the STP state of the port is Disabled if STP 802.1d compliance mode is enabled. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

Spanning Tree port mode

With the STP port mode feature, a switch port can maintain participation in an STP if the port is moved from one VLAN to another. When the STP port mode is configured to auto and a port which does not belong to any VLAN is added to a VLAN, the STP participation of the port is automatically enabled. If the STP port mode is configured to normal and a port which does not belong to any VLAN is added to a VLAN, the STP participation of the port is disabled. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

SSH enhancement to support RSA

When you select the RSA certificate option for a Secure Shell connection to the switch for a client PC, RSA public-private key encryption using a digital certificate with SSH login, is supported as a background option.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

SSHv2

Avaya Ethernet Routing Switch 3500 Series uses the Secure Shell (SSH) version 2 for secure remote logon and other secure network services over an insecure network. SSHv2 can replace Telnet to provide secure access to the user console menu and ACLI interface. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

Static Routing with default route

Default routes specify a route to all networks for which there are no explicit routes in the Forwarding Information Base or the routing table. This static default route is a route to the network address 0.0.0.0 as defined by the IEEE RFC1812 standard.

The Ethernet Routing Switch 3500 Series uses the default route 0.0.0.0/0.0.0.0 for all Layer 3 traffic that does not match a specific route. This traffic is forwarded to the next-hop IP address specified in the default route. For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — IP Routing/Multicast*, NN47203–502.

Sticky MAC

Sticky MAC address provides a high level of control and simpler configuration and operation for MAC address security. Sticky MAC address secures the MAC address to a specified port so that if the address moves to another port, the system raises an intrusion event. When you use Sticky MAC address, the switch performs initial auto-learning of MAC addresses and can store the automatically-learned addresses across switch reboots.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

Syslog

System Log (syslog) displays messages obtained from system Non Volatile Random Access Memory (NVRAM) or Dynamic Random Access Memory (DRAM). The System Log displays only the data for the Avaya Ethernet Routing Switch 3500 Series through the Console or Comm port or Telnet. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

TACACS+

The Avaya Ethernet Routing Switch 3500 Series supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a client/server based protocol that provides centralized validation of users attempting to gain access to a router or network access server.

TACACS+ differs from RADIUS in two important ways:

- TACACS+ is a TCP-based protocol
- TACACS+ uses full packet encryption, rather than only encrypting the password (RADIUS authentication request).

For more information on TACACs+ architecture and feature operation, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

Telnet (up to four sessions)

You can access ACLI through a Telnet session. To access ACLI remotely, the management port must have an assigned IP address and remote access must be enabled. You can log on to the switch using Telnet from a terminal that has access to the Avaya Ethernet Routing Switch 3500 Series.

Multiple users can access ACLI system simultaneously, through the serial port, Telnet, and modems. The maximum number of simultaneous users is four plus one at the serial port for a total of five users on the switch. All users can configure simultaneously.

You can view the Telnet allowed IP addresses and settings, change the settings, or disable the Telnet connection. For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Telnet out (ability to open Telnet sessions from the box)

The Telnet out feature provides a means of creating a telnet session to another host device from the switch CLI.

UDP forwarding

By default, User Datagram Protocol (UDP) broadcast frames received on one VLAN are not routed to another VLAN. To allow UDP broadcasts to reach a remote server, the Ethernet Routing Switch 3500 Series supports UDP broadcast forwarding, which forwards the broadcasts to the server through a Layer 3 VLAN interface.

UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address. The packet is sent as a unicast packet to the server.

For more information and examples of UDP forwarding, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — IP Routing/Multicast*, NN47203–502.

Username Password enhancement

The username and password enhancement provides improved security allowing changes to the standard RO/RW login usernames. The local switch/stack username and password is configurable for RO and RW respectively when logging in via serial, telnet or web interfaces. A login screen is presented and requests the username and password, even for local authentication. For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started,* NN47203–301.

Virtual LACP

Many enterprise networks require that trunk links provide subsecond failover to the redundant link after a failure occurs at the local or remote endpoint. This requirement can be met after both ends of the link are informed of any loss of communication.

Virtual Link Aggregation Control Protocol (VLACP), an LACP extension, is a Layer 2 handshaking protocol that provides end-to-end failure detection between two physical Ethernet interfaces. It allows the switch to detect unidirectional or bidirectional link failures. For more information on VLACP, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

VLAN Tagging enhancement

Rather than setting a port to untagged or tagged mode, you can also choose to enable or disable Port VLAN Identifier (PVID) tagging. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Layer 2*, NN47203–500.

WEB HTTP download of ASCII — allows downloading of ASCII configuration files through HTTP

The ASCII Config Download feature lets you upload software or an ASCII configuration file from a personal computer to the Ethernet Routing Switch 3500 Series using the HTTP protocol. This feature does not require a TFTP server. For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Web Quick Start

You can use the Quick Start menu in Enterprise Device Manager to enter the setup mode through a single screen. Use the Quick Start menu to configure the in-band IP Address and netmask, default gateway, read-only and read-write community strings, quick start VLAN, and IPv6 in-band address and IPv6 default gateway.

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

Writemem and save config command

The **`write memory`** and **`save config`** commands copy the current configuration to NVRAM. Both commands are executed in ACLI in Privileged EXEC command mode. There are no parameters or variables with either command.

For more information, see, NN472*Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

Chapter 3: Important notices

Important notices

This section provides important software and hardware related notices.

File names for this release

The following table describes the Avaya Ethernet Routing Switch 3500 Series, Software Release 5.0, software files. File sizes are approximate.

Module or file type	Description	File name	File size (bytes)
Standard (non-SSH) runtime image software version 5.0.0	Standard software image for the Avaya Ethernet Routing Switch 3500 Series	3500_500008.img	7746420
Secure (SSH) runtime image software version 5.0.0	Standard software image for the Avaya Ethernet Routing Switch 3500 Series	3500_500009s.img	7965044
Boot/Diagnostic software version 1.0.0.4	Diagnostics software for the Avaya Ethernet Routing Switch 3500 Series	3500_1004_diag.bin	2183233
POE firmware version 4.1.0_B4	Power over Ethernet firmware for the Avaya Routing Ethernet Routing Switch 3500 Series	3500_poe_410B4.bin	16384
Software Release 5.0 MIB definition files	Management Information Base (MIB) definition files	Ethernet_Routing_Switch_35xx_MIBs_5.0.0.zip	1309623
EDM Help file zip	A downloadable zip file containing Help	ers3500v500_HELP_EDM.zip	2251102

Module or file type	Description	File name	File size (bytes)
	information for Enterprise Device Manager (EDM)		
COM Plug in file zip	COM Plug in for Enterprise Device Manager (EDM)	ers3500v5.0.0.0..zip	3312924

Upgrading the Diag image using ACLI

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

Procedure

1. Connect a default switch to a TFTP server.
2. Set a valid IP address and subnet mask.
3. Configure the TFTP server address using the following command from Privileged EXEC mode:
   ```
   tftp-server <A.B.C.D>
   ```
4. Verify the connection to the TFTP Server.
5. At the command prompt, enter the **`download`** command with the following parameters.
   ```
   download diag <WORD>
   ```
   The Diag image is downloaded and then the switch is rebooted. To avoid rebooting the switch after the download, add the option <*no-reset*> to the **`download`** command.

Variable definitions

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

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

Updating the Diag image from the Boot menu

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

Procedure

1. Connect a default switch to a TFTP server.
2. Reboot the switch (either a soft or hard reset).
3. During the boot process, press `CTRL+C` until the following menu is displayed:
    a. Press `'a'` to run Agent code.
    b. Press `'d'` to download the agent/diag/bootloader code.
    c. Press `'e'` to display Errors.
    d. Press `'i'` to initialize config flash.
    e. Press `'p'` to run POST tests.
    f. Press `'r'` to reset the switch.
4. Press `'d'`.
5. Choose `option: 2 – Diagnostics`.
6. Choose `option: 1 — Download via TFTP`.
7. Enter the filename, along with its extension; for example `ERS3500_d1_0_0_2.bin`
8. Enter the TFTP server IP address.
9. Enter the switch IP address.
10. Enter the subnet mask.
11. Enter the port in which the cable is connected.
    The download of the DIAG image begins.

Supported software and hardware capabilities

The following table summarizes the known capabilities for the Avaya Ethernet Routing Switch 3500 Series software release 5.0.

Table 2: Supported capabilities for the Avaya Ethernet Routing Switch 3500 Series

Feature	Maximum number supported
QoS egress queues	4
QoS filters per precedence	256
QoS precedence	4
Total QoS filters	(4 x 256) = 1024
MAC addresses	16000
Layer 2	
VLANs	256
Spanning Tree Groups in STPG and RSTP modes	1
Multiple Spanning Tree Instances (MSTI) in MSTP mode	8
MultiLink Trunking (MLT), Link Aggregation (LAG) groups	6
Links for each MLT or LAG	4
Layer 3	
ARP entries (local, static & dynamic)	512 (of which 32 are reserved for local ARPs)
Local ARP Entries (local IP interfaces)	32
Static ARP entries	256
Dynamic ARP entries	max 480 (shares 480 entries with dynamic ARPs)
IPv4 route entries (local, static & dynamic)	32 local + 32 static + 0 dynamic
Static routes and Non-local Static routes	32
Local routes	32
Management routes	4
UDP Forwarding entries	128
DHCP relay entries	256
DHCP relay forward paths	256
Miscellaneous	
802.1X EAP scaling (clients for each port)	32
ADAC (IP Phones)	16
Jumbo frame support	9 K bytes

Feature	Maximum number supported
IGMP multicast groups	up to 59
802.1X (EAP) clients per port, running in MHMA	32
802.1X (EAP) clients per switch	384
LLDP Neighbors	160 on ERS 3510GT 416 on ERS 3524GT 448 on ERS 3526T
RMON alarms	400
RMON events	400
RMON Ethernet statistics	128 per unit
RMON Ethernet history	196 per unit

Supported standards, RFCs and MIBs

Standards

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

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

- IEEE 802.3af (Power over Ethernet — PoE (15.4W))
- IEEE 802.3at (Power over Ethernet plus— PoE+ (32W))

RFCs and MIBs

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

- RFC 783 Trivial File Transfer Protocol (TFTP)
- RFC 791/ 950 Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 826 Address Resolution Protocol (ARP)
- RFC 854 Telnet Server and Client
- RFC 951/ 1542 (BOOTP
- RFC 1112 Internet Group Management Protocol v1 (IGMPv1)
- RFC 1213 MIB-II
- RFC 1215 SNMP Traps Definition
- RFC 1271 / 1757 / 2819 RMON
- RFC 1361 / 1769 Simple Network Time Protocol (SNTP)
- RFC 1493 (Bridge MIB)
- RFC 1573 / 2863 Interface MIB
- RFC 1643 / 2665 Ethernet MIB
- RFC 1905 / 3416 SNMP
- RFC 1906 / 3417 SNMP Transport Mappings
- RFC 1907 / 3418 SNMP MIB
- RFC 1945 HTTP v1.0
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2011 SNMP v2 MIB for IP
- RFC 2012 SNMP v2 MIB for TCP
- RFC 2013 SNMP v2 MIB for UDP
- RFC 2138 RADIUS
- RFC 2236 Internet Group Management Protocol v2 (IGMPv2)
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IPv6

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

Chapter 4: Known issues and limitations

Known issues and limitations

Use the information in this section to learn more about known issues and limitations.

Where appropriate, use workarounds provided for the known issues.

Known issues

The following table lists and describes known issues and limitations for Avaya Ethernet Routing Switch 3500 Series Software Release 5.0. Where available and appropriate, workarounds are provided.

Reference number	Description
WI00966215 WI00966455 WI00968425	**Precedence:** The ASIC has only four slices (precedences) for all the ports. All these slices are occupied by default (one used by ARP, two by QoS and one by DHCP). In order to enable ADAC/IPSG/UDP Fwd, at least one precedence should be freed. The precedences used by QoS can be freed by issuing the following commands: **`“(config)# qos if-group name class trusted”`** **`“(config)# qos if-assign port all name”`** The precedence used by DHCP can be freed by issuing the following command: **`“(config-if)# no ip dhcp-relay”`** Note that the precedence used by ARP cannot be freed.
WI00986612	**IGMP Snooping:** A maximum of 59 IGMP groups is supported by the hardware, not 240 groups as previously reported.
WI00990398	**Port Mirroring:** Packets generated by the CPU (such as BPDU, SONMP and LLDP packets) are not mirrored.
WI00988287	**ASCII config file:** There is a difference between ACLI and EDM in how an ASCII config file is executed on all platforms. When encountering an error, EDM stops the execution and the operation fails, whereas ACLI moves to the next command.

Reference number	Description
WI00988662	**ssh:** The default SSH parameters cannot be modified from a SSH session using ASCII configuration.
WI00988195	**sftp syslog:** Saving the binary configuration to an external TFTP or SFTP server will generate a `bsnConfigurationSavedToNvram` message in the Syslog as the configuration is saved in the NVRAM prior sending it.
WI00990895	**IPSG:** Do not enable IP Source Guard (IPSG) on trunk ports.
WI00984443	**Fan Failure:** If an ERS 3510GT-PWR+ fan fails, during diagnostics, the Status LED should flash Amber, but the Power LED lights Amber instead.
WI00990836	**ACG file download from EDM:** At this time, users should download the configuration using ACLI only.