

Avaya Ethernet Routing Switch 3500 Series Getting Started

© 2013 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/
LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

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

4 Getting Started March 2013

<u>Comments? infodev @avaya.com</u>

Contents

Chapter 1: Purpose	
Chapter 2: New in this release	11
Chapter 3: Getting started fundamentals	17
ACLI commands	
Quick Start	18
Configuring with Quick Start using ACLI	19
BootP automatic IP configuration and MAC address	20
BootP or Default IP	21
BootP Always	21
BootP Disabled	22
BootP or Last Address	22
Default BootP setting	22
Choosing a BootP request mode	22
Asset ID configuration	23
Configuring the Asset ID using ACLI	23
Chapter 4: Connecting to the switch	25
Connecting a terminal to the switch	25
Configuring the terminal	27
Chapter 5: Configuring the management IP address	29
Setting the IP address	
Changing subnet netmask value	30
Setting default gateway	30
Displaying IP configuration	31
Displaying IP address information	32
Chapter 6: Configuring Telnet	35
Setting Telnet access	35
Displaying Telnet access current settings	35
Configuring Telnet access	36
Using ping	38
Chapter 7: Configuring the switch using ACLI	41
Resetting the switch to default configuration	
Using Configuration files	41
Displaying the current configuration	42
Domain Name Server (DNS)	44
Displaying the DNS domain name	44
Pinging the host	45
Configuring the IP address of a DNS server	45
Setting the systems DNS domain name	46
Autosave feature	47
Displaying autosave status	47
Configuring Autosave	48
Displaying ACLI settings	48
Displaying system information	
Customizing the opening banner.	50

	Displaying the current banner	
	Customizing the opening ACLI banner	. 51
	Displaying interfaces	. 52
	Displaying interfaces	52
	Displaying current status of interfaces	54
	Simple Network Time Protocol (SNTP)	. 55
	Displaying SNTP information	55
	Enabling or disabling SNTP	56
	Setting SNTP server primary secondary address	56
	Forcing a Manual Synchronization with NTP Server	. 57
	Setting up recurring synchronization	. 57
	Setting SNTP parameters to default	. 58
	Setting local time zone	. 58
	Setting or disabling clock time zone	. 58
	Setting or disabling daylight savings time	59
	Specifying summer-time recurring dates	. 60
	Displaying the local time zone settings	61
	Displaying the daylight savings time settings	62
	Setting boot parameters using ACLI	62
	Performing a soft-start of the switch	. 63
	Configuring BootP on the current instance of the switch or server	63
Ch	apter 8: Configuring a TFTP server	65
	Setting TFTP parameters	. 65
	Displaying the default TFTP server	. 65
	Assigning or clearing the TFTP address	. 65
Ch	apter 9: Managing Ethernet ports using ACLI	67
	Autosensing and autonegotiation	
	Custom Autonegotiation Advertisements	. 67
	Enabling Custom Autonegotiation Advertisement (CANA) in ACLI	
	Displaying the current autonegotiation advertisements in ACLI	
	Enabling or disabling a port	70
	Naming ports	. 71
	Setting port speed	
	Specifying duplex operation for a port	73
	High speed flow control	
	Symmetric mode	74
	Asymmetric mode	
	Enabling flow control using ACLI	
	Rate limiting configuration	
	Configuring rate limiting using ACLI	
Ch	apter 10: Managing Power Over Ethernet (PoE)	
	Configuring PoE switch parameters	. 79
	Setting the method to detect power devices	
	Setting a power usage threshold	
	Enabling or disabling PoE traps	
	Displaying PoE configuration	. 81
	Displaying the current PoE configuration	21

	Displaying PoE port status	82
	Displaying PoE power measurement	83
	Configuring PoE power mode using ACLI	85
	Displaying Poe power mode using ACLI	86
Cha	pter 11: Upgrading switch software	87
	Upgrading software using ACLI	87
	Upgrading switch software	87
	Show software status	89
	Displaying the agent and image software load	89
Cha	pter 12: Shutting down and resetting a switch	91
	Shutting down the switch	
	Reloading remote devices	92
Cha	pter 13: Configuring the switch using EDM	95
	Configuring Quick Start using EDM	95
	Configuring remote access using EDM	96
	Viewing switch information using EDM	97
	Configuring rate limiting using EDM	98
	Configuring system parameters using EDM	99
	Configuring the Asset ID using EDM	102
	Selecting the ACLI banner type using EDM	102
	Customizing ACLI banner using EDM	103
	Changing switch software using EDM	
	Viewing the agent and image software load status using EDM	106
	Configuring SNTP using EDM	
	Configuring local time zone using EDM	
	Configuring daylight savings time using EDM	
	Configuring recurring daylight saving time using EDM	112
Cha	pter 14: Managing Power over Ethernet (PoE) using EDM	115
	Managing switch PoE using EDM	
	Viewing PoE information for switch ports using EDM	117
	Configuring PoE power mode using EDM	118

Chapter 1: Purpose

This document provides basic instructions to perform the basic configuration of the Avaya Ethernet Routing Switch 3500 Series chassis and software.

Purpose

Chapter 2: New in this release

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

The Avaya ERS 3500 Series is new and supports the following hardware and software features:

ERS 3500 hardware

The following table lists and describes the supported hardware for ERS 3500 Series 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

3 Note:

All switches support autopolarity.

Table 1: Hardware

Hardware	Description
Switch models	
AL3500?01-E6	3526T — 24 10/100BaseT ports supporting autosensing and autonegotiation, 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.
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

Hardware	Description	
	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.	

ERS 3500 software features

The following software features are supported on the ERS 3500 Series Release 5.0:

- BootP or Default IP
- RADIUS password fallback
- Downloading agent & diags without reset
- Username Password enhancement
- Autosave configuration enhancements
- Ping enhancement
- Writemem and save config command
- Configurable SNMP trap port (only SNMP v1 & v2)
- SNTP & SNTP timezone enhancement
- Shutdown, reload enhancement
- Factory-default command
- Show MAC address enhancement
- Show Port enhancement
- Show Running Config (verbose, non-verbose, module) enhancement

- VLAN Tagging enhancement
- 802.1AB (LLDP) Standards Based Auto Topology
- 802.1w&s rapid and multiple spanning trees
- 802.3ad- Link Aggregation Control Protocol (LACP)
- 802.3af Power over Ethernet (PoE)
- 802.3at Power over Ethernet plus (PoE+)
- COS/DSCP allows mapping the DSCP value (carried by IP frames) to 802.1p priority value
- Rate Limiting
- Remote logging ability to log on remote servers
- Web Quick Start
- WEB HTTP download of ASCII allows downloading of ASCII configuration files through HTTP
- HTTP web-based management
- HTTPS/SSL secure web management
- HTTP port change
- CLI Quick Start script
- Auto save Disable
- Telnet (up to four sessions)
- Telnet out ability to open Telnet sessions from the box
- Domain Name Service (DNS) capability
- 256 port-based VLANs with IVL VLAN 1 is the default management VLAN
- 802.1Q tagging
- 802.1p traffic class support / remarking
- Advanced QoS (traffic classification, filtering, mark/remarking, metering, shaping)
- Avaya Automatic-QoS
- Single 802.1d Spanning Tree Protocol (STP) on all ports
- Spanning Tree port mode
- Spanning Tree 802.1d compliance mode
- Port mirroring (1–1)
- Multi-Link Trunking (MLT) with up to six trunks and four links per trunk
- MLT enable/disable whole trunk
- IGMP Multicast no flood command enhancements
- IGMPv1/v2 snooping / proxy
- IGMPv3 Snooping/proxy
- MAC address based security with autolearn (BaySecure)

- Sticky MAC
- RADIUS-based security
- TACACS+
- Local password protection
- SNMPv3 security
- SNMP-based network management
- SNMP MIB web page in EDM
- SNMP Trap list web page in EDM
- Extended IP Manager (IPv4 & IPv6)
- IPv6 Management
- IPv6 VLANs (protocol based)
- No Banner & CTRL-Y Skip
- Local console via serial interface
- 802.3x (Flow Control Gig ports only)
- BootP/TFTP for downloading software and config file
- RMON (RFC1757): per port Statistics, History, Alarm and Events
- ASCII file configuration
- Syslog
- Dual Syslog servers
- ASCII Config Generator (ACG)
- 802.1X EAP (SHSA, MHMA, MHSA, Guest VLAN, Non-EAP & RADIUS MAC)
- 802.1X Enhancement: Dynamic VLAN assignment for NEAP & MHMA
- 802.1X Enhancement: Unicast request, Non-EAP IP Phone support
- 802.1X RFC3576 RADIUS auth extensions CoA
- 802.1X RFC2866/2869 RADIUS interim accounting updates
- 802.1X NEAP with VLAN names
- 802.1X NEAP last assigned VLAN
- 802.1X NEAP fail-open VLAN
- 802.1X NEAP re-authentication timer
- 802.1X NEAP and Guest VLAN on same port
- RADIUS EAP / NEAP to different servers
- RADIUS Server reachability
- DA Filtering
- Port Naming

- CANA
- SSHv2
- SSH enhancement to support RSA
- Secure FTP (SFTP)
- Auto Detection And Configuration (ADAC) with 802.1AB interaction
- 802.1AB MED (Cisco IP Phones)
- 802.1AB Location TLV
- 802.1AB and ADAC interoperability
- 802.1AB Integration features
- 802.1AB Customization features
- Identify Units (Blink LEDs)
- Cumulative system uptime (hidden command)
- Virtual LACP
- Static Routing with default route
- IP Local and Non-Local static routing
- BootP/DHCP Relay
- Proxy ARP
- UDP forwarding
- DHCP Snooping
- DHCP Client
- DHCP Option 82
- Dynamic ARP Inspection
- IP Source Guard
- BDPU Filtering
- MAC flush
- Software Exception Log
- CPU & Memory Utilization
- Configure Asset ID
- Show environmental
- Show software status

New in this release

Chapter 3: Getting started fundamentals

ACLI commands

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 used 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.

You can use ACLI interactively or use the configure network command to load and execute ACLI scripts, manually loading the script in the console menu or automatically loading the script at startup.

ACLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration

If no password is set, you can enter ACLI in User EXEC mode and use the enable command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

User Executive mode is the default ACLI command mode and the initial access mode. Also known as exec mode, it is the most restrictive ACLI mode with only basic commands available; for example, show, ping and logout. User Executive commands are available from the other modes.

Privileged Executive mode is an unrestricted mode that can display all switch settings. If you are logged on with write access, you can access all configuration modes and commands that affect switch operation from Privileged Executive mode.

In Privileged Executive mode, also known as privExec mode, you can perform basic switch level management tasks; for example, downloading software images, setting passwords, and

starting the switch. Privileged Executive commands are also available in Global and Interface configuration modes.

Global Configuration mode, also known as config mode, provides commands used to set and display general switch configurations such as IP address, Simple Network Management Protocol (SNMP) parameters, Telnet access, and Virtual Local Area Networks (VLAN).

Interface Configuration mode, also known as if config mode, provides commands used to configure parameters for each port or VLAN such as speed, duplex mode, and rate limiting.

With sufficient permission, you can use the rules in the following table to move between the command modes.

Command mode and sample prompt	Entrance commands	Exit commands
User Executive 3526T>	No entrance command, default mode	exit or logout
Privileged Executive 3526T#	enable	exit or logout
Global Configuration 3526T <config>#</config>	From Privileged Executive mode, enter configure	To return to Privileged Executive mode, enter end or exit To exit ACLI completely, enter logout
Interface Configuration 3526T <config-if>#</config-if>	From Global Configuration mode: To configure a port enter interface fastethernet <port number=""> To configure a VLAN enter interface vlan <vlan number=""></vlan></port>	To return to Global Configuration mode, enter exit To return to Privileged Executive mode, enter end To exit ACLI completely, enter logout

Quick Start

You can use the install command in Avaya Command Line Interface (ACLI) or the Quick Start menu in Enterprise Device Manager (EDM) to configure the in-band IP Address and

netmask, default gateway, read-only and read-write community strings, quick start VLAN,IPv6 in-band address, and IPv6 default gateway.

Configuring with Quick Start using ACLI

The Install Script consists of a series of prompts that are used to set up the minimum configuration information.

You must enter the following information when prompted:

- IP address
- Subnet mask
- Default gateway
- · Read-only community string
- Read-write community string
- Quick start VLAN

Before you begin

• Connect to the switch using the terminal or terminal emulation application.

Procedure

```
    Press
    CTRL + Y to obtain a CLI prompt.
```

- 2. Enter enable
- Enter install
 The ERS 3500 setup utility banner appears.
- 4. Enter the IP address at the following prompt:

 Please provide the in-band IP Address [0.0.0.0]:
- 5. Enter the sub-net mask at the following prompt:

 Please provide the in-band sub-net mask [0.0.0.0]:
- 6. Enter the default gateway IP address at the following prompt:

 Please provide the Default Gateway [0.0.0.0]:
- 7. Enter the read only community string at the following prompt:

 Please provide the Read-Only Community String [*********]:
- 8. Enter the read write community string at the following prompt::

 Please provide the Read-Write Community String [*********]:
- 9. Enter the VLAN ID for the Quick Start at the following prompt:

 Please provide the Quick Start VLAN <1-4094> [1]:

10. Enter the in-band IPv6 address at the following prompt:

```
Please provide the in-band IPV6 Address/Prefix_length
[ : :/0]:
```

11. Enter the in-band IPv6 default gateway at the following prompt:

```
Please provide the in-band IPV6 Default Gateway [ : :]:
```

Successful completion displays the following message: Basic switch parameters have been configured and saved.

Example

```
Welcome to the 3526T-PWR+ setup utility.
You will be requested to provide the switch basic connectivity settings.
After entering the requested info, the configuration will be applied and
stored into the switch NVRAM.
Once the basic connectivity settings are applied, additional configuration
can be done using the available management interfaces.
Use Ctrl+C to abort the configuration at any time.
Please provide the in-band IP Address[0.0.0.0]:
Please provide the in-band sub-net mask[0.0.0.0]:
Please provide the Default Gateway[0.0.0.0]:
Please provide the Read-Only Community String[*********]:
Please provide the Read-Write Community String[********]:
Please provide the Quick Start VLAN <1-4094> [1]: Please provide the in-band IPV6 Address/Prefix_length[::/0]:
Please provide the in-band IPV6 Default Gateway[::]:
Basic switch parameters have now been configured and saved.
```

BootP automatic IP configuration and MAC address

The Ethernet Routing Switch 3500 Series has a unique 48-bit hardware address, or MAC address, that is printed on a label on the back panel. You can use this MAC address when you configure the network BootP server to recognize the Ethernet Routing Switch 3500 Series BootP requests. A properly configured BootP server lets the switch automatically learns its assigned IP address, subnet mask, IP address of the default router (default gateway), and software image file name.

BootP or Default IP

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

- 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 configured IP address.
- If the configured IP address is 0.0.0.0 or the default IP 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.

BootP Always

This option lets you manage the switch that is configured with the IP address obtained from the BootP server. The Ethernet Routing Switch 3500 Series operates in the BootP Always mode as follows:

- The switch continues to broadcast BootP requests, regardless of whether an in-band IP address is set from the console terminal.
- If the switch receives a BootP reply that contains an in-band IP address, the switch uses this new in-band IP address.
- If the BootP server is not reachable, you cannot change the in-band IP address until the BootP mode is set to BootP Disabled. However, after a period of a few minutes (approximately 10 minutes), the switch automatically enters the BootP Disabled mode. You can then configure the IP address with ACLI.

If an IP address is not currently in use, these actions take effect immediately. If an IP address is currently in use, these actions take effect only after the switch is reset or power cycled.

BootP Disabled

This option lets you manage the switch by using the IP address set from the console terminal. The Ethernet Routing Switch 3500 Series operates in the BootP Disabled mode as described in the following steps:

- The switch does not broadcast BootP requests, regardless of whether an IP address is set from the console terminal.
- The switch can be managed only by using the in-band switch IP address set from the console terminal.

BootP or Last Address

This option lets you manage the switch even if a BootP server is not reachable. The Ethernet Routing Switch 3500 Series operates in the BootP or Last Address mode as described in the following steps:

- When you specify the IP data from the console terminal, the IP address becomes the inband address of the switch. BootP requests are not broadcast. You can manage the switch using this in-band IP address.
- When you do not specify the in-band IP address from the console terminal, the switch broadcasts BootP requests until it receives a BootP reply containing an in-band IP address. If the switch does not receive a BootP reply that contains an in-band IP address within 10 minutes, the switch uses the last in-band IP address it received from a BootP server. This IP information is displayed in the Last BootP column.

If the IP address specified as the in-band IP address is not currently in use, these actions take effect immediately. If an IP address is currently in use, these actions take effect only after the switch is reset or power cycled.

Default BootP setting

The default operational mode for BootP on the switch is BootP or Default IP. The switch requests an IP address from BootP only if one is not already set from the console terminal (or if the IP address is the default IP address: 192.168.1.1).

Choosing a BootP request mode

The BootP Request Mode field lets you choose which method the switch uses to broadcast BootP requests:

- BootP or Default IP
- BootP Always
- BootP Disabled
- BootP or Last Address

Important:

Whenever the switch is broadcasting BootP requests, the BootP process eventually times out if a reply is not received. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes:

- always
- default-ip
- disable
- last

Asset ID configuration

Asset ID provides inventory information for the switch. An Asset ID consists of an alphanumeric string of up to 32 characters in length for the switch. You can configure the Asset ID to record your company specific asset tracking information, such as an asset tag affixed to the switch. You can configure the Asset ID with ACLI commands, or with EDM.

Configuring the Asset ID using ACLI

Configure the Asset ID of a switch to identify the switch using your company-specific inventory or asset tracking information.

Procedure

- 1. Logon to the ACLI Global Configuration Mode.
- 2. At the command prompt, enter the following command:

```
[no] [default] asset-id [unit <1-8>] <WORD>
```

3. Verify the Asset ID:

show system

Variable definitions

The following table describes the parameters for the asset-id command.

Variable	Value
unit <1-8>	Configures the Asset ID of a specific unit. Enter unit number 1–8.
WORD	Specifies the Asset ID which corresponds to your asset tracking system. Enter an alphanumeric Asset ID of up to 32 characters.
no	Removes the Asset ID of a specific unit. Enter a unit number 1–8.
default	Returns the Asset ID of a specific unit to the default value. Enter a unit number 1–8.

Chapter 4: Connecting to the switch

Connecting a terminal to the switch

This procedure describes the steps to connect a terminal to the console port on the ERS 3500 Series switch.

Before you begin

• Terminal with AC power cord and keyboard. Any terminal or PC with an appropriate terminal emulator can be used as the management station. Refer to *Avaya Ethernet Routing Switch 3500 Series Quick Install Guide*, NN47203–300 for a list of the terminal emulation settings that must be used with any terminal emulation software used to connect to the switch.

PEC Code	Short Description	
AL2011020-E6	Avaya DB-9 RED	Avaya RED DB-9 FEMALE TO RJ-45 ADAPTOR. Note: converts the DB-9 MALE to RJ-45 serial port. Can be used for PC or device with DB-9 MALE console port. Can be used with Category 5 RJ-45 straight cable to provide console connection.
AL2011021-E6	Avaya DB-9 BLUE	AVAYA BLUE DB-9 MALE to RJ-45 ADAPTOR. Note: converts DB-9 FEMALE to RJ-45 serial port. Can be used to convert DB-9 of AL2011013–E6 console cable to RJ-45. A Category 5 RJ-45 straight cable can then connect tot RJ-45 console port.
AL2011022-E6	Avaya RJ-45 Console Cable	AVAYA RJ-45/DB-9 INTEGRATED CONSOLE CABLE Note: 1.5m cable with DB-9 Female for PC and RJ-45 for device console port.

• Use the following RJ-45 console cables to connect the switch console port to your management terminal. The maximum length for the console port cable is 25 feet (8.3 meters).

Refer to Avaya Ethernet Routing Switch 3500 Series Quick Install Guide, NN47203-300 for console port pin-out information. You can use the pin-out information to verify or create a console cable for use with your maintenance terminal.

Procedure

- 1. Connect one end of the serial cable to the connector on the terminal or PC.
- 2. Connect the other end of the serial cable to the console port on the switch.
- 3. Turn the terminal or PC on.
- 4. Set the terminal protocol on the terminal or terminal emulation program to VT100 or VT100/ANSI.
- 5. Connect to the switch using the terminal or terminal emulation application. The Avaya switch banner appears when you connect to the switch through the console port.
- 6. Enter Ctrl+Y and type the following CLI commands:

enable

install

The setup utility prompts you to enter the information requested.

```
Welcome to the 3526T-PWR+ setup utility.
You will be requested to provide the switch basic connectivity settings. After entering the requested info, the configuration will be applied and
stored into the switch NVRAM.
Once the basic connectivity settings are applied, additional configuration
can be done using the available management interfaces.
Use Ctrl+C to abort the configuration at any time.
Please provide the in-band IP Address[0.0.0.0]:
Please provide the in-band sub-net mask[0.0.0.0]:
Please provide the in-band sub-net mask[0.0.0.0]:
Please provide the Default Gateway[0.0.0.0]:
Please provide the Read-Only Community String[*********]:
Please provide the Read-Write Community String[*********]:
Please provide the Quick Start VLAN <1-4094> [1]:
Please provide the in-band IPV6 Address/Prefix_length[::/0]:
Please provide the in-band IPV6 Default Gateway[::]:
Basic switch parameters have now been configured and saved.
```

Figure 1: Setup Utility

Configuring the terminal

You can configure the switch terminal settings to suit your preferences for the terminal speed and display.

About this task

Use the following procedure to configure terminal settings including the terminal connection speed, and terminal display width and length, in number of characters.

Procedure

- 1. Logon to the ACLI User EXEC mode.
- 2. At the command prompt, enter the following command:

```
terminal speed \{2400 | 4800 | 9600 | 19200 | 38400\} | length <1-132> | width <1-132>
```

3. To display the current serial port information, enter the following command: show terminal

Example

The following figure shows the output from the show terminal command.

```
3510GT-PWR> enable
3510GT-PWR# show terminal
Terminal speed: 9600
Terminal width: 79
Terminal length: 23
```

3510GT-PWR#

Variable definitions

The following table describes the parameters for the terminal command.

Variable	Value
speed {2400 4800 9600 19200 38400}	Sets the transmit and receive baud rates for the terminal. You can set the speed to one of the five options shown. DEFAULT: 9600
length <1-132>	Sets the length of the terminal display in characters. RANGE: 1 to 132

Connecting to the switch

Variable	Value
	DEFAULT: 24
width <1-132>	Sets the width of the terminal display in characters. RANGE: 1 to 132 DEFAULT: 79

Chapter 5: Configuring the management IP address

Setting the IP address

Use this procedure to set the IP address and subnet mask for the switch, clear the existing IP address and subnet mask, or return the IP address and subnet mask to the default value.

! Important:

When you change the IP address or subnet mask, you can lose connection to Telnet and the Web. You also disable any new Telnet connection, and you must connect to the serial Console port to configure a new IP address.

Procedure

- 1. Log on to the ACLI Global Configuration mode.
- 2. At the command prompt, enter the following command:

[default] [no] ip address <A.B.C.D> [netmask <A.B.C.D>]

Variable definitions

The following table describes the parameters for the ip address command.

Variable	Value
A.B.C.D	Enters the IP address or subnet mask of the switch in the format XXX.XXX.XXXX; netmask is optional.
netmask	Sets the IP subnet mask for the switch
default	Sets the IP address for the specified unit to the default value of 192.168.1.1.
no	Clears the IP address and subnet mask; this changes the IP address and submask mask for a switch to all zeros (0).

Changing subnet netmask value

The subnet mask is set using procedure <u>Setting the IP address</u> on page 29. Use this procedure to change the subnet mask to the default value or clear the subnet mask.

Procedure

- 1. Log on to the ACLI Global Configuration mode.
- 2. At the command prompt, enter the following command:

```
[default] [no] ip netmask
```

Variable definitions

The following table describes the parameters for the ip netmask command.

Variable	Value
default	Sets the subnet mask to the default value (255.255.255.0).
no	Sets the subnet mask for a switch to all zeros (0.0.0.0).

Setting default gateway

Use this procedure to set the IP default gateway address for a switch, change the IP default gateway address to the default address, or clear the IP default gateway address.

! Important:

When you change the IP gateway address, you can lose connection to Telnet and the Web. You also can disable any new Telnet connection required to connect to the serial Console port to configure a new IP Gateway address.

Procedure

- 1. Log on to the ACLI Global Configuration mode.
- 2. At the command prompt, enter the following command:

[no] [default] ip default-gateway

Variable definitions

The following table describes the parameters for the ip default-gateway command.

Variable	Value
<a.b.c.d></a.b.c.d>	Enter the IP address of the default IP gateway in the format XXX.XXX.XXX.XXX. DEFAULT: 0.0.0.0.
	1 Important:
	When you change the IP gateway, you can lose connection to Telnet and the Web. You can also disable any new Telnet connection required to connect to the serial Console port to configure a new IP Gateway address.
no	Clears the IP address of the default IP gateway. Sets the IP default gateway address to zeros (0).
default	Sets the IP default gateway address to all zeros (0.0.0.0).

Displaying IP configuration

This procedure is used to display the IP configuration, specifically BootP mode, switch address, subnet mask, and gateway address. These parameters are displayed for what is configured, what is in use, and the last BootP.

Procedure

- 1. Logon to the ACLI in User EXEC command mode.
- 2. At the command prompt, enter the following command:
 show ip [bootp] [default-gateway] [address [switch]] [dns]

If you do not enter any parameters, the **show ip** command displays all IP-related configuration information.

Example

The following figure displays a sample output of the **show** ip command.

Variable definitions

The following table describes the parameters for the **show** ip command.

Variable	Value
bootp mode	Displays BootP-related IP information
default-gateway	Displays the IP address of the default gateway
address	Displays the current IP address
switch	Specifies the current IP address of the switch
dns	Displays the DNS configuration

Displaying IP address information

Use this procedure to display the IP configurations, switch address, subnet mask, and gateway address.

Procedure

- 1. Log on to the ACLI User EXEC command mode.
- 2. At the command prompt, enter the following command:

show ip address

Example

The following figure displays a sample output for the show ip address command.

3524GT-PWR+(config)#	show ip address		
	Configured	In Use	Last BootP/DHCP
Switch IP Address:	172.16.120.10	172.16.120.10	0.0.0.0
Switch Subnet Mask:	255.255.255.0	255.255.255.0	0.0.0.0
3524GT-PWR+(config)#			

Configuring the management IP address

Chapter 6: Configuring Telnet

Setting Telnet access

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.

! Important:

Multiple users can access the ACLI system simultaneously, through a 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.

Displaying Telnet access current settings

Display the current settings for Telnet access.

Procedure

- 1. Log on to the ACLI Privileged EXEC command mode.
- 2. At the command prompt, enter the following command:

```
show telnet-access
```

Example

The following figure displays sample output for the show telnet-access command.

```
2 255.255.255.255
                               255.255.255.255
3
   255.255.255.255
                               255.255.255.255
   255.255.255.255
                               255.255.255.255
5
   255.255.255.255
                               255.255.255.255
  255.255.255.255
                               255.255.255.255
   255.255.255.255
                               255.255.255.255
8
   255.255.255.255
                               255.255.255.255
   255.255.255.255
                               255.255.255.255
10 255.255.255.255
                               255.255.255.255
11 255.255.255.255
                               255.255.255.255
12 255.255.255.255
                               255.255.255.255
13 255.255.255.255
                               255.255.255.255
14 255.255.255.255
                               255.255.255.255
----More (q=Quit, space/return=Continue)----
```

Configuring Telnet access

Configure the Telnet connection that is used to manage the switch.

Procedure

- 1. Log on to ACLI Global Configuration mode.
- 2. At the command prompt, enter the following command:

```
[no] [default] telnet-access [enable|disable] [logon-timeout
<1-10>] [retry <1-100>] [inactive-timeout <0-60>] [logging
{none|access|failures|all}] [source-ip <1-10> <A.B.C.D>[mask
<A.B.C.D>]]
```

Variable definitions

The following table describes the parameters for the telnet-access command.

Variable	Value
enable disable	Enables or disables Telnet connections
logon-timeout <1–10>	Specifies the time in minutes that you want to wait between an initial Telnet connection and acceptance of a password, before closing the Telnet connection; enter an integer between 1 and 10.
retry <1-100>	Specifies the number of times that the user can enter an incorrect password before closing the connection; enter an integer between 1 and 100.

Variable	Value
inactive-timeout <0-60>	Specifies in minutes how long to wait before closing an inactive session; enter an integer between 0 and 60.
logging none access failures all	Specifies what types of events you want to save in the event log:
	All — Saves all access events in the log:
	- Telnet connect — indicates the IP address and access mode of a Telnet session
	- Telnet disconnect — indicates the IP address of the remote host and the access mode, due to either a log off or inactivity.
	 Failed Telnet connection attempts — indicates the IP address of the remote host that is not on the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password.
	none — No Telnet events are saved in the event log.
	access — Connect and disconnect events are saved in the event log.
	failure — Only failed Telnet connection attempts are saved in the event log.
source-ip <1–10> <a.b.c.d>[mask <a.b.c.d>]</a.b.c.d></a.b.c.d>	Specifies up to 10 IP address from which connections are allowed. Enter the IP address either as an integer or dotted-decimal notation (A.B.C.D in the format XXX.XXX.XXX.XXX). Specifies the subnet mask from which connections are allowed; enter the IP mask in dotted-decimal notation (A.B.C.D in the format XXX.XXX.XXX.XXXX)
	Important:
	These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see Avaya Ethernet Routing Switch 3500 Series-Configuration — Security, NN47203–504.
no telnet-access [source-ip [<1-10>]]	Disables the Telnet connection. When you do not use the optional parameter, the source-

Variable	Value
	up list is cleared, meaning that the 1st index is set to 0.0.0.0/0.0.0.0 and the 2nd to 10th indexes are set to 255.255.255.255.255.255.255.255. When you do specify a source-ip value, the specified pair is set to 255.255.255.255.255.255.255.255.255.
	Important:
	These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see Avaya Ethernet Routing Switch 3500 Series-Configuration — Security, NN47203–504.
default	Sets the Telnet settings to the default values.

Using ping

To ensure that the Ethernet Routing Switch 3500 Series has connectivity to the network, ping a device you know is connected to this network. 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. For more information about setting IP addresses, see Setting the IP address on page 29.

Before you begin

The local IP address must be set before issuing the ping command.

Procedure

- 1. Log on to ACLI in User EXEC command mode.
- 2. At the command prompt, enter the following command:

```
ping <A.B.C.D>[datasize <64-4096>] [{count <1-9999>} |
continuous] [{timeout | -t} <1-120>] [interval <1-60>]
[debug]
```

If the device receives the packet, it sends a ping reply. When the switch receives the reply, it displays a message indicating that the specified IP address is being

used. If no reply is received, a message indicates that the address is not responding.

Example

The following figure shows a sample ping response.

3510GT-PWR+#ping 120.16.125.10 Host is reachable 3510GT-PWR+#

Variable definitions

The following table describes the parameters for the ping command.

Variable	Value
ping <a.b.c.d hostname="" or=""></a.b.c.d>	Specifies the IP address of the target device in dotted-decimal notation (A.B.C.D in the format XXX.XXX.XXX.XXX).
datasize<64-4096>	Specifies the size of the ICMP packet to be sent. The data size range is from 64 to 4096 bytes.
{count <1-9999>} / continuous	Sets the number of ICMP packets to be sent. The continuous mode sets the ping running until the user interrupts it by entering Ctrl-C.
{timeout -t} <1-120>	Sets the timeout using either the timeout or -tparameter, followed by the number of seconds the switch must wait before timing out.
interval<1-60>	Specifies the number of seconds between transmitted packets.
debug	Provides additional output information such as ICMP sequence number and trip time.

Configuring Telnet

Chapter 7: Configuring the switch using ACLI

Resetting the switch to default configuration

Reset the switch to its factory default configuration.

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command: restore factory-default [-y | force]
- 3. The -y or force parameter instructs the switch not to prompt for confirmation. If the -y or force parameter is not included in the command, the following message appears: Warning the switch will be reset to factory default configurationDo you wish to continue (y/n)?

 Enter y to restore the swtich to default.

Using Configuration files

Configuration files allow the administrator to change switch configuration quickly. You can display, store, and retrieve configuration files, and save the current configuration.

The Configuration management feature lets you store and retrieve the configuration parameters of an Ethernet Routing Switch 3500 Series to a TFTP server and retrieve the parameters to automatically configure a replacement switch. This feature supports two different methods for managing system configuration files:

- binary configuration files
- ASCII configuration files

Before you change the switch configuration, you can use the **show running-config** command to view the current configuration. The command displays only those parameters that

differ from the default switch configuration. If you want to view the entire configuration, you must use the verbose qualifier to view the configuration for a specific feature.

A configuration file obtained from a stand-alone switch can only be used to configure other stand-alone switches that have the same firmware revision and model type as the donor stand-alone switch.

The following parameters are not saved to the configuration file:

- Configuration Image Filename
- Terminal settings (speed, width, length)

Refer to Avaya Ethernet Routing Switch 3500 Series — Fundamentals, NN47203–102, for procedures on

- Viewing current configuration using ACLI
- Saving current configuration using ACLI
- Saving current configuration to flash memory using ACLI
- Restoring system configuration from TFTP using ACLI
- Downloading a configuration file automatically using ACLI
- Storing current ASCII configuration on a TFTP server using EDM
- Downloading an ASCII configuration from a TFTP server using EDM
- Downloading a configuration file automatically using EDM
- Storing a binary configuration file on a TFTP server using EDM
- Downloading a binary configuration file on a TFTP server using EDM
- Saving current configuration to flash memory manually using EDM

Displaying the current configuration

Display the current configuration of the switch.

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command: show running —config [verbose] [module <value>]

! Important:

If the switch CPU is busy performing other tasks, the output of the **show running-config** command can appear to intermittently stop and start. This is

normal operation to ensure that other switch management tasks received appropriate priority.

Example

The following figure provides a sample of the **show running-config** command with the MLT value.

```
ERS-3524T# show running-config module mlt
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 3524T
! Software version = v5.0.0.22
! Displaying only parameters different to default
enable
configure terminal
! *** MLT (Phase 1) ***
no mlt
mlt 1 name "Trunk #1" enable member 11-14
mlt 1 bpdu single-port
mlt 1 loadbalance advance
mlt 2 name "Trunk #2" enable member 21-24
! *** MLT (Phase 2) ***
mlt spanning-tree 1 stp learning fast
mlt spanning-tree 2 stp learning disable
ERS-3524T#
```

Variable definitions

The following table describes the optional parameters for the **show running-config** command.

Variable	Value
verbose	Displays entire configuration, including defaults and non-defaults.
module <value></value>	Displays configuration of an application for any of the following parameters: [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]

Variable	Value
	[poe] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [ssh] [ssl] [stp] [vlacp] [vlan]

Domain Name Server (DNS)

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.

You can also 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.

Displaying the DNS domain name

Display the DNS domain name, as well as any configured servers.

Procedure

- Log on to ACLI in User Exec command mode.
- 2. At the command prompt, enter the following command: show ip dns

Example

The following figure provides a sample of the **show ip dns** command.

```
3524GT-PWR+(config)#show ip dns
DNS Default Domain name: None

DNS Servers
-----
0.0.0.0
0.0.0.0
0.0.0.0
3524GT-PWR+(config)#
```

Pinging the host

You can test the network connection to another network device using the ping command. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device.

You can ping a host using either its IP address or hostname.

Before you begin

A local IP address must be set before issuing the ping command.

Procedure

- 1. Log on to ACLI in User Exec command mode.
- 2. At the command prompt, enter the following command: ping <A.B.C.D or Hostname>

Variable definitions

The following table describes the parameters for the ping command.

Variable	Value
<a.b.c.d hostname="" or=""></a.b.c.d>	Specifies:
	the IP address of the target device in dotted-decimal notation (A.B.C.D in the format XXX.XXX.XXXX)
	the hostname of the device to ping. The hostname can be a simple name, such as fred; in this case the DNS domain name, if set, is appended. Or the hostname can be a full hostname, such as fred.ca.avaya.com.
	DEFAULT: none

Configuring the IP address of a DNS server

Add or remove one or more DNS servers' IP addresses. You can add or remove up to three servers; one at a time.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

Variable definitions

The following table describes the parameters for the ip name-server command.

Variable	Value
<a.b.c.d></a.b.c.d>	Specifies the IP address of a DNS server to be added or removed in the format XXX.XXX.XXX.XXX. DEFAULT: 0.0.0.0
no	Removes the specified DNS server name.

Setting the systems DNS domain name

Specifies the DNS domain name for the Avaya Ethernet Routing 3500 Series switch.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

Variable definitions

The following table describes the parameters for the ip domain-namecommand.

Variable	Value
<line></line>	Specifies the system's DNS domain name. DEFAULT: empty string
no	Clears the system's DNS domain name (sets it to an empty string).

Variable	Value
default	Clears the system's DNS domain name (sets it to an empty string).

Autosave feature

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.

! Important:

Do not power off the switch within 60 seconds of changing configuration parameters. Doing so causes loss of changes in the configuration parameters.

You can enable or disable the autosave feature using the autosave enable and no autosave enable commands.

You can use ACLI command copy config nvram to force a manual save of the configuration when the autosave feature is disabled.

Displaying autosave status

Display the status of the autosave feature, either enabled or disabled.

Before you begin

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command: show autosave

Example

The following figure provides a sample of the show autosave command.

3524-PWR+(config)#show autosave Auto Save: Enabled 3524-PWR+(config)#

Configuring Autosave

The Ethernet Routing Swtich 3500 Series performs a check every 60 seconds to detect changes to the configuration file or a new log message in the nonvolatile storage. If any of these events occurs, the switch automatically saves its configuration and the nonvolatile log to flash memory. Autosave also automatically saves your configuration information following restarts.

You can enable or disable the Autosave feature. After you disable autosave, changes in the configuration file are not saved to the flash memory.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
[no] [default] autosave enable
```

Variable definitions

The following table describes the parameters for the autosave enablecommand.

Variable	Value
no	Disables the autosave feature.
default	Returns the autosave feature to the default value. DEFAULT: Autosave Enabled

Displaying ACLI settings

Display the current ACLI settings such as general console settings, ACLI mode, ACLI user names and passwords, and password types.

Procedure

- 1. Log on to ACLI in User EXEC command mode.
- 2. At the command prompt, enter the following command:

```
show cli {info | mode | password [type]}
```

Example

The following figure provides a sample of the show cli command.

```
3524GT-PWR+(config)#show cli info
Inactivity Timeout: 15 minute(s)
Login Timeout: 1 minute(s)
Login Retries: 3
More: True
Screen Lines: 23
3524GT-PWR+(config)#
```

Variable definitions

The following table describes the parameters for the **show** cli command.

Variable	Value
info	Displays general Console settings
mode	Displays ACLI mode
password	Displays ACLI user names and passwords
type	Displays password types

Displaying system information

Display the current system characteristics.

! Important:

You must enable and configure SNTP to display GMT time. Refer to <u>Simple Network Time</u> <u>Protocol (SNTP)</u> on page 55 for more details.

Before you begin

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command:

show sys-info

Example

The following figure provides a sample of the show sys-info command.

```
3524GT-PWR+(config) #show sys-info
Operation Mode:
MAC Address:
                              C8-F4-06-D7-C8-00
POE Module FW:
                             4.0.1B2
                             16
Reset Count:
Last Reset Type:
                             Software Download
                             Enabled
Autotopology:
                            None
Pluggable Port 21:
Pluggable Port 22:
                            None
                            None
Pluggable Port 23:
                            None
Pluggable port 24:
Pluggable Port 25:
                             None
                         None
Pluggable Port 26:
                            Ethernet Routing Switch 3524GT-PWR+
sysDescr:
                            HW:R0B FW:t1116 SW:v5.0.0.045
                            Mfg Date: 20111101 HW Dev:none
Operational Software: FW:t1116 SW:v5.0.0.045
Installed software: FW: SW:v5.0.0.045
Operational license: Base software
Installed license: Base software
sysObjectID:
Serial #:
                             SDNI24GTP0B001
sysObjectID:
                              1.3.6.1.4.1.45.3.80.4
sysUpTime:
                             8 days, 08:58:56
sysNtpTime:
                            NTP not synchronized
sysServices:
sysContact:
sysName:
----More (q=Quit, space/return=Continue)----
```

Customizing the opening banner

You can customize the banner that appears when you connect to the Ethernet Routing Switch 5000 Series. You can customize the text that reads AVAYA. However you cannot customize the second line that reads Enter [Ctrl]+y to begin.

The Banner Control feature provides an option to specify the banner text. If you choose not to display the banner, the system enters the ACLI command mode through the default command interface. You do not have to press the Ctrl+y keys.

The Banner display that you select is used for subsequent console sessions. For executing the new mode in the console, you must logout. For Telnet access, all subsequent sessions use the selected mode.

Displaying the current banner

Display the current banner.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
show banner [custom | static]
```

Variable definitions

The following table describes the parameters for the **show banner** command.

Variable	Value
static	Displays default banner
custom	Displays custom banner
(if empty)	Displays static, custom or disabled status if parameter is not entered

Customizing the opening ACLI banner

Specifies the banner displayed at startup; either static or custom.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
[no] banner [custom | static | disabled | <1-19> LINE ]
```

Variable definitions

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

Variable	Value
static	Displays the default agent-banner
custom	Displays the custom agent-banner
disabled	Skips the agent-banner display
<1–19> LINE	Fills the Nth line of the custom banner (1 <n<19) in="" line<="" specified="" td="" text="" the="" with=""></n<19)>

Variable	Value
no	Clears all lines of a previously stored custom banner

Displaying interfaces

You can view the status of all interfaces on the switch, including MultiLink Trunk membership, link status, autonegotiation, and speed.

Displaying interfaces

Display the current configuration and status of all interfaces.

Procedure

- 1. Log on to ACLI in User Exec command mode.
- 2. At the command prompt, enter the following command: show interfaces [names | gbic-info] [<portlist>] [verbose]

Example

The following figure provides a sample of the **show interfaces** command with the *names* variable.

```
3510GT(config)#show interfaces name 1 3
Port Name
---- ----
1 LabBldg
2 Testing
3 FloorBldg
```

The following figure shows a sample output of the **show interfaces** command without the *names* variable.

35240	GT-PWR+(config)#		terface	es				
		Stat	us			Auto			Flow
Port	Trunk	Admin	Oper	Link	LinkTrap	Negotiation	Speed	Duplex	Control
1		Enable	Down	Down	Enabled	Enabled			
2		Enable	Up	Up	Enabled	Enabled	100Mk	ps Full	Symm
3		Enable	Down	Down	Enabled	Enabled			
4		Enable	Down	Down	Enabled	Enabled			
5		Enable	Down	Down	Enabled	Enabled			
6		Enable	Down	Down	Enabled	Enabled			
7		Enable	Down	Down	Enabled	Enabled			
8		Enable	Down	Down	Enabled	Enabled			
9		Enable	Down	Down	Enabled	Enabled			
10		Enable	Down	Down	Enabled	Enabled			
11		Enable	Down	Down	Enabled	Enabled			

```
Enable Down Down Enabled Enabled

Enable Down Down Enabled Enabled
```

The following figure shows a sample output of the **show interfaces** command with the *verbose* variable.

```
35324-PWR+(config)#show interfaces verbose
Port:
    Trunk:
    Admin Status: Enable
    Oper Status: Down
    EAP Oper Status: Down
    VLACP Oper Status: Down
    STP Oper Status: Discarding
    Link: Down
    LinkTrap: Enabled
    Link Autonegotiation: Enabled
    BPDU-guard (BPDU Filtering): Disabled
    BPDU-guard (BPDU Filtering): Oper Status: N/A
Port: 2
    Trunk:
    Admin Status: Enable
    Oper Status: Up
    EAP Oper Status: Up
    VLACP Oper Status: Down
    STP Oper Status: Forwarding
    Link: Up
    LinkTrap: Enabled
    Link Autonegotiation: Enabled
----More (q=Quit, space/return=Continue)----
```

Variable definitions

The following table describes the parameters for the **show interfaces** command.

Variable	Value
gbic-info	Displays Gigabit Interface Converter (GBIC) details
LINE	Displays the interface information for specific ports
names	Displays the interface names
<portlist></portlist>	Specifies the port number(s) to be displayed
verbose	Requests full information about each port

Displaying current status of interfaces

Display the current operational status of interfaces and provide supplementary information about the current port settings for Spanning Tree Protocol.

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command:

```
show interfaces [<portlist>] config
```

Example

The following figure provides a sample of the **show interfaces config** command.

```
35324-PWR+(config)#show interfaces 10-14 config
Port:
        10
    Trunk:
    Admin Status: Enable
    Oper Status: Down
    EAP Oper Status: Up
    VLACP Oper Status: Down
    STP Oper Status: Discarding
    Link: Down
    LinkTrap: Enabled
    Link Autonegotiation: Enabled
    BPDU-guard (BPDU Filtering): Disabled
    BPDU-quard (BPDU Filtering): Oper Status: N/A
Port:
    Trunk:
    Admin Status: Enable
    Oper Status: Down
    EAP Oper Status: Up
    VLACP Oper Status: Down
    STP Oper Status: Discarding
    Link: Down
    LinkTrap: Enabled
    Link Autonegotiation: Enabled
----More (q=Quit, space/return=Continue)----
```

Variable definitions

The following table describes the parameters for the **show interfaces** config command.

Variable	Value
<pre><portlist.></portlist.></pre>	Enter the ports you want to display.

Simple Network Time Protocol (SNTP)

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.

The system retries connecting with the NTP server a maximum of 3 times, with 5 minutes between each retry. If the connection fails after the 3 attempts, the system waits for the next synchronization time (the default is 24 hours) and begins the process again.

! Important:

If you have trouble using this feature, try various NTP servers. Some NTP servers may be overloaded or currently inoperable.

Displaying SNTP information

Display the SNTP information, as well as the configured NTP servers.

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command:

show sntp

Example

The following figure provides a sample output of the show sntp command.

```
3524GT-PWR+(config)#show sntp
                               Disabled
SNTP Status:
Primary server address:
                              0.0.0.0
Secondary server address:
                              0.0.0.0
Sync interval:
                               24 hours
Last sync source:
                               0.0.0.0
Primary server sync failures:
Secondary server sync failures: 0
Last sync time:
                               Not Set
Next sync time:
                               Not Set
Current time:
                               Not Set
3524GT-PWR+(config)#
```

Enabling or disabling SNTP

Enable or disable Simple Network Time Protocol . The default value for SNTP is Disabled.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command (without the optional [no] parameter to enable SNTP:

[no] sntp enable

Variable definitions

The following table describes the parameters for the **sntp enable** command.

Variable	Value
no	Disables SNTP

Setting SNTP server primary secondary address

Set or clear the IP address for the primary or secondary NTP server.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

[no] sntp server <primary|secondary> address <A.B.C.D>

Variable definitions

The following table describes the parameters for the sntp server condary>address command.

Variable	Value
<a.b.c.d></a.b.c.d>	Enter the IP address of the primary or secondary NTP server in the format XXX.XXX.XXXX.XXX.

Variable	Value
	DEFAULT: 0.0.0.0.
no	Clears the NTP server IP addresses
<pre><primary secondary></primary secondary></pre>	Enter the NTP server you want to set or clear:
	primary — the IP address for the primary NTP server
	secondary — the IP address for the secondary NTP server

Forcing a Manual Synchronization with NTP Server

Force a manual synchronization with the NTP Server. This procedure is useful if the recurring synchronization is long, and you want to correct or test the operation immediately, rather than waiting for, or changing the reoccurrence period.

Before you begin

You must enable SNTP before this procedure can be performed.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command: sntp sync-now

Setting up recurring synchronization

You can specify recurring synchronization with the NTP server in hours, relative to the initial synchronization.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

sntp sync-interval <0-168>

Variable definitions

The following table describes the parameters for the sntp sync-interval command.

Variable	Value
<0–168>	Specifies the number of hours you want for periodic synchronization with the NTP server.
	0- synchronization at start-time only
	• 168 — once a week
	DEFAULT: 24 hours

Setting SNTP parameters to default

Setting the SNTP parameters to their default values allows you to disable SNTP, clear stored SNTP server addresses, and restore the default SNTP synchronization interval.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command: default sntp [enable | server | sync-interval]

Setting local time zone

Simple Network Time Protocol (SNTP) uses Universal Coordinated Time (UTC) for all time synchronizations so it is not affected by different time zones. In order for the switch to report the correct time for your local time zone and daylight savings time, you must set local time zone and summer time zone (if using Daylight Savings Time).

Setting or disabling clock time zone

Set the local time zone relative to Universal Coordinated Time (UTC), or disable the clock time zone feature.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
[no] clock time-zone <zone> <hours> <minutes>
```

Variable definitions

The following table describes the parameters for the clock time-zone command.

Variable	Value
zone	Specifies time zone acronym that can be displayed when showing system time; for example, EST for Eastern Standard Time. RANGE: Up to 4 characters
hours	Specify the hours difference from UTC. RANGE: —12 to + 12
minutes	Optional minutes difference from UTC. RANGE: 0–59
no	Disables the clock time zone feature

Setting or disabling daylight savings time

Set the daylight savings time with start and end dates, or disable the daylight savings time feature.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
[no] clock summer-time <zone> [date {<day> <month> <year>
<hh:mm>} {<day> <month> <year> <hh:mm>}] [<offset>]
```

Variable definitions

The following table describes the parameters for the clock summer-time command.

Variable	Value
zone	Specifies the acronym to be displayed when summer time is in effect. If unspecified, defaults to the time zone acronym. RANGE: up to 4 characters
date { <day> <month> <year> <hh:mm>} {<day> <month> <year> <hh:mm>}</hh:mm></year></month></day></hh:mm></year></month></day>	The first date specifies when summer time starts, and the second date specifies when summer time ends.
	• day — day of the month (RANGE: 1 to 31)
	month — month (RANGE: first three letters by name)
	hh:mm — time in military format (24–hour clock), in hours and minutes
	Important:
	<day> <month> parameters can also be entered in order: <month> <day>.</day></month></month></day>
offset	Number of minutes to add during summer time RANGE: —840 to 840
no	Disables the daylight savings time feature

Specifying summer-time recurring dates

Specify the dates that recur during the summer-time clock every year. This procedure provides flexibility for countries where the Daylight Savings Time is different than North America.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

clock summer-time recurring <1-5> <DAY> <MONTH> hh:mm> <1-5>
<DAY> <MONTH> <hh:mm> <1-1440>

Example

The following figure provides a sample of the output of the clock summer-time recurring command.

```
3526T(config)#clock summer-time recurring 1 tues Jun 12:01 3 sat Sep 23:57 1
Summer time recurring is set to:
start: 1st week of June on Tuesday at 12:01
end: 3rd week of September on Saturday at 23:57
Offset: 60 minutes.
3526T(config)#
```

Variable definitions

The following table describes the parameters for the summer-time recurring command.

Variable	Value
<1–5>	Specifies the week of the month. The first occurrence specifies when the recurring starts, and the second specifies when the recurring stops.
<day></day>	Specifies the day of the week as the first 3 letters of the name. The first occurrence specifies when the recurring starts, and the second specifies when the recurring stops.
<month></month>	Specifies the Month using the first 3 letters of the name. The first occurrence specifies when the recurring starts, and the second specifies when the recurring stops.
<hh:mm></hh:mm>	Specifies the time in hours and minutes in military format (24–hr). The first occurrence specifies when the recurring starts, and the second specifies when the recurring stops.
<1–1440>	Specifies the number of minutes to add or subtract during summer-time recurring.

Displaying the local time zone settings

Display the settings for the local time zone.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
show clock time-zone
```

Example

The following figure provides a sample of the output of the show clock time-zone command.

```
3524GT-PWR+(config)#show clock time-zone
Time zone offset from UTC is 00:00
3524GT-PWR+(config)#
```

Displaying the daylight savings time settings

Display the daylight savings time settings.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
show clock summer-time
```

Example

The following figure provides a sample of the output of the show clock summer-time command.

```
3524GT-PWR+(config)#show clock summer-time
Summer time recurring is set to:
start: on Tuesday in the 1st week of June at 12:01
end: on Saturday in the 3rd week of September at 23:59
Offset: 60 minutes.
Daylight saving time is disabled
3524GT-PWR+(config)#
```

Setting boot parameters using ACLI

You can restart the switch and configure BootP using ACLI.

Performing a soft-start of the switch

Use this command to perform a soft-start of the switch.

Procedure

- 1. Logon to the Privileged EXEC mode in ACLI.
- 2. To perform a soft-start of the switch, enter the following command: boot [default]

Variable definitions

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

Variable	Value
default	Restores switch to factory-default settings after restarting.

Configuring BootP on the current instance of the switch or server

Use this command to configure BootP on the current instance of the switch or server, as the default ip, the last known address, never, or always.

Procedure

- 1. Logon to the Global Configuration mode in ACLI.
- 2. To configure BootP on the current instance of the switch or server, enter the following command:

```
[no] [default] ip bootp server {default-ip|last|disable|
always]
```

Variable definitions

The following table describes the parameters for the ip bootp server command.

Variable	Value
default-ip last disable always	Specifies when to use BootP:
	default-ip — use BootP or the default IP
	last — use BootP or the last known address
	disable — never use BootP
	always — always use BootP
	DEFAULT: default-ip
no	Disables the BootP server
default	Sets the BootP server status to BootP or Default IP

Chapter 8: Configuring a TFTP server

Setting TFTP parameters

You can display the IP address of the TFTP server and assign an IP address to the TFTP server.

For procedures to copy a configuration file to the TFTP server, or copy a configuration file from the TFTP server to the switch to use to configure the switch, refer to *Avaya Ethernet Routing Switch 3500 Series — Fundamentals*, NN47203–102.

Displaying the default TFTP server

Display the IP address of the server used for all TFTP-related transfers.

Before you begin

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command:

```
show tftp-server
```

Example

The following figure provides a sample output of the show tftp-server command.

```
3524GT-PWR+>enable
3524GT+#show tftp-server
TFTP Server IP address: 172.16.3.2
```

Assigning or clearing the TFTP address

Assign or clear the address for the switch to use for TFTP services.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

Variable definitions

The following table describes the parameters for the tftp-server command.

Variable	Value
<a.b.c.d></a.b.c.d>	Specifies the dotted-decimal IP address of the server you want to use for TFTP services in the format XXX.XXX.XXX.XXX.
no	Clears the TFTP server IP address to 0.0.0.0.
default	Sets the TFTP server IP address to 0.0.0.0.

Chapter 9: Managing Ethernet ports using ACLI

Autosensing and autonegotiation

The Ethernet Routing Switch 3500 Series is an autosensing and autonegotiating device.

- The term autosense refers to the ability of a port to sense the speed of an attached device.
- The term autonegotiation refers to a standardized protocol (IEEE 802.3u) that exists between two IEEE 802.3u-capable devices. Autonegotiation lets the switch select the best of speed and duplex modes.

Autosensing is used when the attached device is not capable of autonegotiation or is using a form of autonegotiation that is not compatible with the IEEE 802.3u standard. In this case, because it is not possible to sense the duplex mode of the attached device, the Ethernet Routing Switch 3500 Series reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the Ethernet Routing Switch 3500 Series, the ports negotiate down from 1000 Mb/s speed and full-duplex mode (ERS 3510GT and ERS 3524GT) and from 100 Mb/s speed and full-duplex mode (ERS 3526T) until the attached device acknowledges a supported speed and duplex mode.

Custom Autonegotiation Advertisements

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 releases, 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.

In certain situations, it is useful to autonegotiate a specific speed and duplex value. In these situations, the switch can allow for attachment at an operating mode other than its highest supported value.

For example, if the switch advertises only a 100 Mbps full-duplex capability on a specific link, the link goes active only if the neighboring device is also capable of autonegotiating a 100 Mbps full-duplex capability. This prevents mismatched speed and duplex modes if customers disable autonegotiation on the neighboring device.

! Important:

The CANA feature is available for 10/100 Ethernet ports of ERS 3526T switches, and 10/100/1000 ports on the ERS 3510GT and ERS 3524GT switches (not available for rear ports).

Enabling Custom Autonegotiation Advertisement (CANA) in ACLI

You can control the capabilities that are advertised by the Ethernet Routing Switch as part of the auto-negotiation process using the Custom Autonegotiation Advertisements (CANA) feature. After autonegotiation is disabled, the hardware is configured for a single (fixed) speed and duplex value. After auto-negotiation is enabled, the advertisement made by the switch is a constant value based upon all speed and duplex modes supported by the hardware. After auto-negotiating, the switch selects the highest common operating mode supported between it and its link partner.

Displaying the current autonegotiation advertisements in ACLI

Use this command to display the current autonegotiation advertisements.

Procedure

- 1. Logon to the User EXEC mode in ACLI.
- 2. To display the current autonegotiation advertisements, enter the following command:

show auto-negotation-advertisements [port <portlist>]

Example

3526T(config-if)#show auto-negotiation-advertisements port 2,4,8

Port Autonegotiation Advertised Capabilities

2 10Full 10Half 100Full 100Half 1000Full Pause
4 10Full 10Half 100Full 100Half 1000Full Pause
8 10Full 10Half 100Full 100Half 1000Full Pause
3526T(config-if)#

Variable definitions

The following table describes the parameters for the **show auto-negotiation-advertisements** command.

Variable	Value
port <portlist></portlist>	Enter ports for which you want the current autonegotiation advertisements displayed. If you enter more than one port number, separate ports with a comma (,).

Displaying the hardware advertisement capabilities for the switch in ACLI

Use this command to display the hardware advertisement capabilities for the switch.

Procedure

- 1. Logon to the User EXEC mode in ACLI.
- 2. To display the hardware advertisement capabilities for the switch, enter the following command:

show auto-negotiation-capabilities [port <portlist>]

Variable definitions

The following table describes the parameters for the show auto-negotiation-advertisements command.

Variable	Value
port <portlist></portlist>	Enter ports for which you want the current autonegotiation advertisements displayed. If you enter more than one port number, separate ports with a comma (,).

Enabling or disabling a port

Enable or disable a port with ACLI

! Important:

You can disable switch ports that are trunk members, if you choose to disable them one by one. If you choose to disable all ports of the unit, the changes can affect the ports belonging to MLTs.

Procedure

- 1. Log on to ACLI in the Interface Configuration command mode.
- 2. At the command prompt, enter the following command:

[no] shutdown [line <portlist>]

Example

The following figure provides a sample of the output of the **shutdown** [port <portlist>]command.

3524GT<config-if>#shutdown port 6 3524GT<config-if>#

Variable definitions

The following table describes the parameters for the **shutdown** [port <portlist>] command.

Variable	Value
port <portlist></portlist>	Specifies the port numbers to shut down or disable. Enter the port numbers you want to disable.
	Important:
	If you omit this parameter, the system uses the port number you specified in the interface command.
no	Specifies the port numbers to enable. Enter the port number you want to enable.

Variable	Value
	Important: If you omit this parameter, the system uses the port number you specified in the interface command.

Naming ports

You can name ports, change the name, clear the name or reset the port name to an empty string.

Procedure

- 1. Log on to ACLI in Interface Configuration command mode.
- 2. At the command prompt, enter the following command:
 [no] [default] name [port <portlist>] <LINE>

Variable definitions

The following table describes the parameters for the name [port <portlist>] command.

Variable	Value
port <portlist></portlist>	Specifies the port numbers to be named.
	Important:
	If you omit this parameter, the system uses the port number you specified in the interface command.
<line></line>	Specifies the name of the port using up to 26 alphanumeric characters.
no	Clears the port names and resets the field to an empty string.
default	Clears the port names and resets the field to the default value (an empty string).

Setting port speed

Set the speed of a port. Ports can be set to a speed of 10 Mb/s, 100 Mb/s, 1000 Mb/s (or 1 GB/s), or auto-negotiated.

Procedure

- 1. Log on to ACLI in Interface Configuration command mode.

Variable definitions

The following table describes the parameters for the speed [port <portlist>] command.

Variable	Value
default	Sets the speed of the port to the factory default speed.
port <portlist></portlist>	Specifies the port numbers to configure the speed. Enter the port numbers to be configured.
	Important:
	If you omit this parameter, the system uses the port number you specified in the interface command.
10 100 1000 auto	Sets speed to:
	• 10 — 10 Mb/s
	• 100 — 100 Mb/s
	• 1000 — 1000 Mb/s or 1 GB/s
	• auto — autonegotiation
	Important:
	When you set the port speed for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

Specifying duplex operation for a port

Specify duplex operation as full-duplex mode, half-duplex mode, or auto-negotiated. You can also reset duplex operation for a port to the factory default duplex value.

Procedure

- 1. Log on to ACLI in Interface Configuration command mode.
- 2. At the command prompt, enter the following command:
 [default] duplex [port <portlist>] {full|half|auto}

Variable definitions

The following table describes the parameters for the duplex [port <portlist>] command.

Variable	Value
port <portlist></portlist>	Specifies the port number to configure the duplex mode. Enter the port number you want to configure, or ALL to configure all ports simultaneously.
	① Important:
	If you omit this parameter, the system uses the port number you specified in the interface command.
full half auto	Sets duplex to:
	• full — full-duplex mode
	half — half-duplex mode
	• auto — autonegotiation
	Important:
	When you set the duplex mode for autonegotiation, ensure that the other side of the link is also set for autonegotiation.
default	Sets the duplex operation for a port to the factory default duplex value.

High speed flow control

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.

Two high speed flow control modes are available:

Symmetric mode

This mode lets both GBIC port and its link partner to send flow control pause frames to each other.

When a pause frame is received (by either the GBIC port or its link partner), the port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frame is received. Both devices on the link must support this mode when it is selected.

Asymmetric mode

This mode lets the link partner send flow control pause frames to the GBIC port. When a pause frame is received, the receiving port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frame is received.

In this mode, the GBIC port is disabled from transmitting pause frames to its link partner. Use this mode when the GBIC port is connected to a buffered repeater device.

You can choose a flow control mode with ACLI commands.

Enabling flow control using ACLI

If you use a Gigabit Ethernet with the Ethernet Routing Switch 3500 Series, you control traffic on this port using the flowcontrol command.

Before you begin

- Autonegotiation must be set to Disabled on the port.
- The speed/duplex must be 1000/full.

74 Getting Started March 2013

About this task

The **flowcontrol** command is used only on Gigabit Ethernet ports and controls the traffic rates during congestion.

Procedure

- 1. Logon to the Interface Configuration mode in ACLI.
- 2. To configure flow control on Gigabit Ethernet ports, enter the following command: [no] [default] flowcontrol [port <portlist>] {asymmetric| symmetric|auto|disable}

Variable definitions

The following table describes the parameters for the flowcontrol command.

Variable	Value	
port <portlist></portlist>	Specifies the port numbers to use for flow control	
	Important:	
	If you omit this parameter, the system uses the port number you specified in the interface command.	
asymmetric symmetric auto disable	Sets the mode for flow control:	
	asymmetric — enables the local port to perform flow control on the remote port	
	symmetric — enables the local port to perform flow control	
	auto — sets the port to automatically determine the flow control mode	
	disable — disables flow control on the port	
	DEFAULT:auto	
no	Disables flow control on the specified port(s).	
default	Sets the flow control to auto, which automatically detects the flow control on the specified port(s).	

Rate limiting configuration

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.

When the volume of either packet type is high, placing severe strain on the network (often referred to as a "storm"), you can set the forwarding rate of those packet types to not exceed a specified percentage of the total available bandwidth. The pps (Packets Per Second) value you set is a small amount of the maximum value of pps for the maximum available bandwidth that is 262143 pps.

! Important:

All Rate Limiting configuration settings are applied across the entire unit. You cannot set some ports in the unit to limit broadcast traffic with a value of X pps and some other ports in the same to limit multicast traffic with a value of Y pps.

You can view the rate limiting configuration settings and statistics with the **show rate-limit** command or the **show running-config** ACLI command. You can also limit the percentage of multicast traffic, or broadcast traffic, or both with **rate-limit** ACLI command.

Displaying rate-limit configuration using ACLI

Display rate-limit configuration to view settings and statistics.

Procedure

- Logon to the ACLI in Privileged EXEC mode.
- 2. At the command prompt, enter the following command: show rate-limit

3.

Example

The following figure displays sample output from the show rate-limit command.

3510GT-PWR+show rate-limit Packet Type Limit

```
-----Both 0 pps
3510GT-PWR+#
```

Configuring rate limiting using ACLI

Configure rate limiting in packets per second for the specified traffic type: either multicast, broadcast, or both.

Procedure

- 1. Logon to the ACLI Global Configuration Mode.
- 2. At the command prompt, enter the following command: [no] [default] rate-limit [multicast|broadcast|both] <0-262143>

Variable definitions

The following table describes the parameters for the rate-limit command.

Variable	Value
multicast broadcast both	Applies rate limiting, in packets/second, to the specified type of traffic:
	multicast — applies rate limiting to multicast packets
	broadcast — applies rate limiting to broadcast packets
	both — applies rate limiting to both multicast and broadcast packets
<0-262143>	Sets the pps (Packets Per Second) upper threshold limit for the traffic type. When the volume of packets exceeds this threshold, packets are dropped. The pps value you set is a small percent of the maximum value of pps for the total available bandwidth (262143 pps).
no	Disables rate limiting on the switch
default	Restores the default value for rate limiting for the switch

Managing Ethernet ports using ACLI

Chapter 10: Managing Power Over Ethernet (PoE)

Configuring PoE switch parameters

You configure power parameters for each Ethernet Routing Switch 3500–PWR+ with ACLI. You can configure the DC power source and the power usage with this management system.

Setting the method to detect power devices

Set the method the Ethernet Routing Switch 3500–PWR+ uses to detect the power devices connected to the front ports.

You must ensure that this setting is the correct one for the IP appliance you use with the switch. Please note this setting applies to the entire switch, not port-by-port. So, you must ensure that this setting is configured correctly for all the IP appliances on a specified switch.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
poe poe-pd-detect-type {802dot3af | 802dot3af_and_legacy |
802dot3at | 802dot3at_and_legacy}
```

Variable definitions

The following table describes the parameters for the poe poe-pd-detect-type command.

Variable	Value
802dot3af 802dot3af_and_legacy 802dot3at 802dot3at_and_legacy	Sets the detection method the switch uses to detect power needs of devices connected to the front ports:

Variable	Value
	• 802dot3af
	802dot3af_and_legacy
	• 802dot3at
	802dot3at_and_legacy
	DEFAULT: 802dot3af_and_legacy
	Important:
	Ensure that the power detection method you choose for the ERS 3500–PWR+ matches that used by the IP devices you are powering.

Setting a power usage threshold

Set a percentage usage threshold above which the system sends a trap for each Ethernet Routing Switch 3500–PWR+

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

poe poe-power-usage-threshold {<1-99>}

Variable definitions

The following table describes the parameters for the poe poe-power-usage-threshold command.

Variable	Value
<1–99>	Specifies the percentage of total available power you want the switch to use prior to sending a trap. DEFAULT: 80%

Enabling or disabling PoE traps

Enable or disable the traps for the PoE functions on the Ethernet Routing Switch 3500–PWR +.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
[no] snmp-server notification-control
{pethPsePortOnOffNotification |
pethMainPowerUsageOnNotification |
pethMainPowerUsageOffNotification}
```

Variable definitions

The following table describes the parameters for the snmp-server notification-control command.

Variable	Value
pethPsePortOnOffNotification pethMainPowerUsageOnNotification pethMainPowerUsageOffNotification	Specifies a notification type
no	Disables the traps for the PoE function

Displaying PoE configuration

You can display the status for the PoE configuration on the Ethernet Routing Switch 3500–PWR+ using ACLI.

Displaying the current PoE configuration

Display the current PoE configuration of the Ethernet Routing Switch 3500–PWR+, and settings for each PoE port.

- 1. Log on to ACLI in User Exec command mode.
- 2. At the command prompt, enter the following command:

```
show poe-main-status
```

Example

The following figure provides a sample output of the show poe-main-status command.

Important:

The Power Source Present listing displays the current power source for the switch: AC Only.

Displaying PoE port status

Display the administration status, detection status, power limit, port priority, and the PD classification for each port.

The DTE Power Status displays error messages if the port is not providing power. The following messages can appear:

- Detecting port detecting IP device requesting power
- Delivering power port delivering requested power to device
- Invalid PD port detecting device that is not valid to request power
- Deny low priority power disabled from port because of port setting and demands on power budget
- Overload power disabled from port because port is overloaded
- Test port in testing mode
- Error none of the other conditions apply
- Disabled the port has been administratively disabled

- 1. Log on to ACLI in User Exec command mode.
- 2. At the command prompt, enter the following command:

```
show poe-port-status [port <portlist>]
```

Example

The following figure provides a sample output of the show poe-port-status command.

3524GT-PWR+#show poe-port-status						
		Admin Current Limit				
Port	Status	Status	Classification	(Watts)	Priority	
1	Enable	Detecting	0	32	Low	
1 2 3	Enable	Invalid PI	0	32	Low	
3	Enable	Detecting	0	32	Low	
4	Enable	Detecting	0	32	Low	
5	Enable	Detecting	0	32	Low	
6	Enable	Detecting	0	32	Low	
7	Enable	Detecting	0	32	Low	
8 9	Enable	Detecting	0	32	Low	
9	Enable	Detecting	0	32	Low	
10	Enable	Detecting	0	32	Low	
11	Enable	Detecting	0	32	Low	
12	Enable	Detecting	0	32	Low	
13	Enable	Detecting	0	32	Low	
14	Enable	Detecting	0	32	Low	
15	Enable	Detecting	0	32	Low	
16	Enable	Detecting	0	32	Low	
17	Enable	Detecting	0	32	Low	
18	Enable	Detecting	0	32	Low	
19	Enable	Detecting	0	32	Low	
M	More (q=Quit, space/return=Continue)					

Variable definitions

The following table describes the parameters for the show poe-port-status command.

Variable	Value
port <portlist></portlist>	Enter the ports for which you want to display the status. If you omit this parameter, the system displays all ports.

Displaying PoE power measurement

Display the voltage, current and power values for each powered device connected to each port.

- 1. Log on to ACLI in User Exec command mode.
- 2. At the command prompt, enter the following command: show poe-power-measurement [port <portlist>]

Example

The following figure provides a sample output from the **show poe-power-measurement** command.

3524GT-PWR+>enable				
3524GT-PWR+#show poe-power-measurement				
Port	Volt(V)	Curr	ent(mA)	Power(Watt)
1	0.0	0		0.000
2	0.0	0		0.000
3	0.0	0		0.000
4	0.0	0		0.000
5	0.0	0		0.000
6	0.0	0		0.000
7	0.0	0		0.000
8	0.0	0		0.000
9	0.0	0		0.000
10	0.0	0		0.000
11	0.0	0		0.000
12	0.0	0		0.000
13	0.0	0		0.000
14	0.0	0		0.000
15	0.0	0		0.000
16	0.0	0		0.000
17	0.0	0		0.000
18	0.0	0		0.000
19	0.0	0		0.000
20	0.0	0		0.000
More (q=Quit, space/return=Continue)				

Variable definitions

The following table describes the parameters for the **show poe-power measurement** command.

Variable	Value
port <portlist></portlist>	Enter the ports for which you want to display the power measurements. If you omit this parameter, the system displays all ports.

Configuring PoE power mode using ACLI

The ERS 3510GT-PWR+ switch is able to operate in two Power over Ethernet (PoE) budget modes:

- Fanless mode Low Power Mode
- Normal mode High Power Mode

The default is: High Power Mode (Normal mode).

In Fanless mode, the fan is shut down and will not be activated, despite the internal temperature. To prevent the switch from overheating, the PoE budget is limited to 60 Watts. Although the internal temperature may show as High in this mode, the ERS 3510GT-PWR+ switch has been designed to operate at temperatures about 60°C. When the switch is operating in Fanless mode, diagnostic fan tests are not performed and the show environmental command does not display details about the fan.

In Normal mode, the fan operates normally and is activated when the temperature reaches its threshold. See <u>Setting a power usage threshold</u> on page 80. In Normal mode, the PoE budget is not limited; a maximum of 170 Watts is available.

Use the following procedure to set the PoE operating mode to low (Fanless) or high (Normal) power mode.

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
[default] poe power-mode {low-power-budget| high-power-
budget}
```



The switch does not need to reboot for the change in power mode to take effect.

Example

The following figure provides a sample of the poe power-mode command.

```
PoE Main Status - Stand-alone

Power Mode : Low Power Budget

Available DTE Power : 60 Watts

DTE Power Status : Normal

DTE Power Consumption : 0 Watts

DTE Power Usage Threshold : 80 %

PD Detect Type : 802.3at and Legacy

Power Source Present : AC Only
```

```
AC Power Status : Present
DC Power Status : Not Present
```

Variable definitions

The following table describes the parameters for the poe power-mode command.

Variable	Value
low-power-budget high-power-budget	Specifies the power mode:
	low-power-budget — for fanless mode
	high-power-budget — for normal mode
	DEFAULT — high-power-budget (normal mode)
default	Resets the power mode to the default value — normal mode (high-power-budget)

Displaying Poe power mode using ACLI

Use the following procedure to display the poe operating mode. There are 2 power modes; low (Fanless) or high (Normal).

The default is: high power mode (Normal mode).

Procedure

- 1. Log on to ACLI in Global Configuration command mode.
- 2. At the command prompt, enter the following command:

```
show poe poe-main-status
```

Example

The following figure provides a sample of the show poe poe-main-status command.

Chapter 11: Upgrading switch software

Upgrading software using ACLI

You can download the Ethernet Routing Switch 3500 Series software image that is in nonvolatile flash memory. To download the software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the Ethernet Routing Switch 3500 Series must have an IP address.



Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

Upgrading switch software

Upgrade the software for the Ethernet Routing Switch 3500 Series. You can upgrade both the software image and the diagnostics image.

! Important:

The system resets after downloading a new image.

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command:

```
download [address <ip>] {image <image-name>|image-if-newer
<image-name>|diag <filename> [no-reset] | poe-module-image }
```

! Important:

You can use the download command without parameters. The system displays the most recently used TFTP server IP address and file name; if you still want to use these, press Enter. You can also change these.

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Take care not to interrupt the download process until after it runs

to completion (the process can take up to 10 minutes, depending on network conditions.

When the download process is complete, the switch automatically resets and the new software image initiates a self-test. The system returns a message after successfully downloading a new image.

During the download process, the Ethernet Routing Switch 3500 Series is not operational. You can monitor the progress of the download process by observing the LED indications.

Example

The following figure provides a sample output of the download command.

```
3524GT-PWR+>enable
3524GT-PWR+#download
Address [172.16.3.2] :
Filename [3500_500s_041.img] :
Finished Upgrading Image Rebooting
3524GT-PWR+#
```

Variable definitions

The following table describes the parameters for the download command.

Variable	Value
address <ip></ip>	Specifies the IP address of the TFTP server you want to use.
	Important:
	If this parameter is omitted, the system goes to the server specfied by the tftp-server command.
image <image-name></image-name>	Enter the name of the Ethernet Routing Switch 3500 Series software image you want to download.
image-if-newer <image-name></image-name>	Enter the name of the Ethernet Routing Switch 3500 Series software image of the newer version you want to download.
diag <filename></filename>	Enter the name of the Ethernet Routing Switch 3500 Series diagnostic image you want to download.
no-reset	Download the specified software without resetting the unit.
poe-module-image	Specifies the name of the PoE image file.

88 Getting Started March 2013

Show software status

You can display the currently loaded and operational switch software status for both agent and diagnostic loads. You can use the **show** boot ACLI command and variables to display the agent or diagnostic load status individually, or combined.

Displaying the agent and image software load

Display the currently loaded and operational software status for agent and image loads, either individually or combined, for a switch.

Procedure

- 1. Log on to ACLI in User Exec command mode.
- 2. At the command prompt, enter the following command:

```
show boot [diag] [image]
```

Example

The following figure provides a sample output of the show boot command.

```
3524GT-PWR+>show boot
Unit Agent Image Active Image Diag Image Active Diag
----
1# 5.0.0.041 5.0.0.041 t1116
* - Unit requires reboot for new Active Image to be made operational.
# - Unit requires reboot for new Diag to be made operational.
3524GT-PWR+>
```

Variable definitions

The following table describes the parameters for the **show** boot command.

Variable	Value
diag	Displays information for the agent load only.
image	Displays information for the image load only.

Upgrading switch software

Chapter 12: Shutting down and resetting a switch

Shutting down the switch

Use this procedure to safely shut down a switch without interfering with device processes or corrupting the software image. After the **shutdown** 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.

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command: shutdown [force] [minutes-to-wait <1-60>] [cancel]

Variable definitions

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

Variable	Value
force	Forces the shutdown without confirmation.
minutes-to-wait<1-60>	Specifies the number of minutes to wait before the shutdown occurs. DEFAULT: 10
cancel	Cancels a scheduled shutdown any time during the time period specified by the minutes-to-wait <1–60> parameter.

Reloading remote devices

Use this procedure to disable auto saving configuration changes, and safeguard against a configuration error when you perform dynamic configuration changes on a remote switch. If you make an error while configuring a remote switch that results in the loss of connectivity (for example, an error in the IP address, VLAN, etc.), the reload loads the last saved configuration to re-establish connectivity.

This procedure does temporarily disable auto-save functionality until the reload occurs. Cancelling the reload returns auto-save functionality to any previous setting.

Before you begin

This procedure is intended to by used by system administrators to configure remote devices and reset them when the configuration is complete. The configuration is not explicitly saved after the reload command is issued. This means that any configuration changes must be explicitly saved before the switch reloads.



You must perform a timed reload command before making dynamic configuration changes to safeguard against the loss of remote connectivity.

Procedure

- 1. Log on to ACLI in Privileged EXEC command mode.
- 2. At the command prompt, enter the following command:

```
reload [force] [minutes-to-wait <1-60> [cancel]
```

Example

The following example shows use of the reload command as a safeguard during dynamic configuration changes:

- 1. Enter reload force minutes-to-wait 30 to instruct the switch to reboot in 30 minutes and load the configuration from NVRAM. During the 30 minute countdown, autosave of the configuration is disabled.
- 2. Execute dynamic switch configuration commands. The command take effect immediately and are not saved to NVRAM.
- 3. Test your configuration changes. If problems occurred, when the 30 minute countdown expires, the switch reboots and loads the previous configuration. If no problems occur, and switch connectivity is maintained, you can perform one of the following tasks before the 30 minute countdown expires:
- Enter copy config nvramto save the new configuration.
- Enter reload cancel to cancel the previous reload command.

Next steps

Variable definitions

The following table describes the parameters for the reload command.

Variable	Value
force	Forces the reload without confirmation.
minutes-to-wait<1-60>	Specifies the number of minutes to wait before the reload occurs. DEFAULT: 10
cancel	Cancels a scheduled reload any time during the time period specified by the <i>minutes-to-wait <1–60></i> parameter.

Shutting down and resetting a switch

94 Getting Started March 2013

Chapter 13: Configuring the switch using EDM

Configuring Quick Start using EDM

Perform this procedure to configure Quick Start to enter the setup mode through a single screen.

Procedure

- 1. From the navigation tree, click Administration.
- 2. In the Administration Tree, click Quick Start.
- 3. In the In-Band Switch IP address, type a switch address.
- 4. In the In-Band Subnet Mask dialog box, type a subnet mask.
- 5. In the Default Gateway dialog box, type an IP address.
- 6. In the Read-Only Community String box, type a character string.
- 7. In the Re-enter to verify dialog box immediately following the Read-Only Community String box, retype the character string from Step 6.
- 8. In the Read-Write Community String dialog box, type a character string.
- 9. In the Re-enter to verify dialog box immediately following the Read-Write Community String box, retype the character string from Step 8.
- 10. In the Quick Start VLAN dialog box, type a VLAN ID.

11. Click Apply.

Example



Configuring remote access using EDM

Use this procedure to configure remote access for a switch.

Procedure

- 1. In the navigation tree, double-click **Administration**.
- 2. In the Administration tree, click **Remote Access**.
- 3. In the work area, click the **Setting** tab.
- 4. In the Telnet Remote Access Setting section, select a value from the Access list.
- 5. In the Telnet Remote Access Setting section, select a value from the **Use List** list.
- 6. In the SNMP Remote Access Setting section, select a value from the Access list.
- 7. In the SNMP Remote Access Setting section, select a value from the **Use List** list.
- 8. In the Web Page Remote Access Setting section, select a value from the **Use List** list.
- 9. In the SSH Remote Access Setting section, select a value from the **Access** list.
- 10. In the SSH Remote Access Setting section, select a value from the **Use List** list.

11. On the toolbar, click Apply.

Remote Access Setting field descriptions

The following table describes the fields on the Remote Access Setting tab.

Name	Description
Telnet Remote Access Setting	Specifies the remote access settings for telnet sessions:
	Access: Allows or disallows telnet access to the switch
	Use List: Enables (Yes) or disables (No) the use of listed remote Telnet information.
SNMP Remote Access Setting	Specifies SNMP remote access settings:
	Access: Allows or disallows SNMP access to the switch
	Use List: Enables (Yes) or disables (No) the use of listed remote SNMP information.
Web Page Remote Access Setting	Specifies web page remote access settings
	Use List: Enables (Yes) or disables (No) the use of listed remote web page information.
SSH Remote Access Setting	Specifies SSH access settings:
	Access: Allows or disallows SSH access to the switch
	Use List: Enables (Yes) or disables (No) the use of listed remote SSH information.

Viewing switch information using EDM

Use this procedure to display switch specific information such as the type of switch, hardware version number, serial number, the number of base ports, and the total number of ports.

- 1. From the Device Physical View, click a switch.
- 2. From the navigation tree, click **Edit**.
- 3. In the Edit tree, click Unit.

Unit field descriptions

The following table describes the fields on the Unit tab.

Name	Description
Туре	Specifies the type of switch.
Descr	Description of switch.
Ver	Specifies the hardware revision number of the switch.
SerNum	Specifies the serial number of the switch.
BaseNumPorts	Specifies the base number of ports.
TotalNumPorts	Specifies the total number of ports.

Configuring rate limiting using EDM

Use this procedure to display and configure rate limiting on a switch.

Procedure

- 1. From the Device Physical View, click a unit.
- 2. From the navigation tree, click Edit.
- 3. In the Edit tree, click **Unit**.
- 4. In the work area, select the Rate Limit tab.
- 5. To a rate limit, click a TrafficType row.
- 6. Double-click the cell in the **AllowedRatePps** column.
- 7. Type a value.
- 8. Double-click the cell in the Enable column.

- 9. Select a value from the list true to enable the traffic type, or false to disable the traffic type.
- 10. On the toolbar, click **Apply**.

Rate Limit tab field descriptions

The following table describes the fields on the Rate Limit tab.

Name	Description
Traffic Type	Specifies the traffic type.
AllowedRatePps	Allowed traffic rate packets/second. It is in the range of 0–262143.
	Important:
	Rate Limiting feature is disabled when AllowedRatePps is set to 0.
Enable	When Enable is set to True, the TrafficType can either be multicast, broadcast, or both.
	Important:
	You cannot set the Enabled field for both multicast and broadcast TrafficType to False at the same time. This is an illegal configuration.

Configuring system parameters using EDM

Use this procedure to view and modify the system level configuration.

Procedure

- 1. In the navigation tree, click **Edit**.
- 2. In the Edit tree, click Chassis.
- 3. In the Chassis tree, click Chassis.
- 4. In the work are, click the **System** tab.
- 5. In the **sysContact** dialog box, type system contact information.
- 6. In the **sysName** dialog box, type a system name.
- 7. In the **sysLocation** field, type a system location.

- 8. Perform one of the following:
 - To enable authentication traps, select the **Authentication Traps** check box.
 - To disable authentication traps, clear the **Authentication Traps** check box.
- 9. In the **Reboot** section, click a radio button.
- 10. In the AutoPvid section, click a radio button.
- 11. In the **BootMode** section, click a radio button.
- 12. On the toolbar, click Apply.

System tab field descriptions

The following table describes the fields on the System tab.

Name	Description
sysDescr	Provides device specific information. This is a read-only item.
sysUpTime	Indicates the amount of time since the system was last booted.
sysObjectID	Indicates the system object identification number. This is a read-only field.
sysContact	Specifies contact information for the system administrator, which can include a contact name or email address.
sysName	Specifies a unique name to describe this switch.
sysLocation	Specifies the physical location of this device.
SerNum	Indicates the serial number of this switch.
AuthenticationTraps	Enables or disables authentication traps. When enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When disabled, no SNMP traps are received.
Reboot	Options include:
	running: the switch remains in the running mode (default)
	• reboot : initiates a hardware reset.

100 Getting Started March 2013

Name	Description
AutoPVID	When enabled, a VLAN ID can be automatically assigned to any port.
NextBootMgmtProtocol	Indicates the transport protocols to use after the next switch restart. This is a read-only item.
CurrentMgmtProtocol	Indicates the current transport protocols that the switch supports. This is a read-only item.
BootMode	Specifies whether to use the BootP or DHCP server to assign an IPv4 address for the management VLAN at the next switch reboot. Values include:
	other: read only
	bootpDisabled: use configured server IP address
	bootpAlways: always use the BootP server
	bootpWhenNeeded: use the BootP server when necessary
	bootpOrLastAddress: use the BootP server last used
	dhcp: always use the DHCP server
	dhcpWhenNeeded: use the DHCP server when necessary
	dhcpOrLastAddress: use the DHCP server last used
ImageLoadMode	Indicates the source from which to load the agent image at the next boot. This is a read-only items.
CurrentImageVersion	Indicates the version number of the agent image that is currently used on the switch. This is a read-only item.
LocalStorageImageVersion	Indicates the version number of the agent image that is stored in flash memory on the switch. This is a read-only item.
NextBootDefaultGateway	Indicates the IP address of the default gateway for the agent to use after the next time you boot the switch. This is a read-only item.

Name	Description
CurrentDefaultGateway	Indicates the address of the default gateway that is currently in use. This is a read-only item.
NextBootLoadProtocol	Indicates the transport protocol that the agent uses to load the configuration information and the image at the next boot. This is a read-only item.
LastLoadProtocol	Indicates the transport protocol last used to load the image and configuration information about the switch. This is a read-only item.

Configuring the Asset ID using EDM

Use this procedure to configure the Asset ID for a switch.

Procedure

- 1. In the navigation tree, double-click **Edit**.
- 2. In the Edit tree, double-click Chassis.
- 3. In the Chassis tree, click Chassis.
- 4. In the work area, click the **Asset ID** tab.
- 5. In the table, click the cell under the **Asset ID** column heading.
- 6. In the **Asset ID** field, enter an alphanumeric value, up to 32 characters.
- 7. On the toolbar, click Apply.

Selecting the ACLI banner type using EDM

Use this procedure to select the type of banner that is displayed in the Avaya Command Line (ACLI) Telnet screen.

Procedure

- 1. In the navigation tree, click **Edit**.
- 2. In the Edit tree, click Chassis.
- 3. In the Chassis tree, click Chassis.

102 Getting Started March 2013

4. In the work area, select the **Banner** tab.

Banner tab field descriptions

The following table describes the fields on the Banner tab.

Name	Description
BannerControl	Specifies the banner to be displayed when you connect to an Avaya Ethernet Routing Switch 3500 Series device using Telnet. Values include:
	• static: uses a predefined static banner.
	• custom: uses a custom banner.
	disabled : prevents the display of any banner.

Customizing ACLI banner using EDM

Use this procedure to customize the banner that is displayed in the Avaya Command Line (ACLI) Telnet screen. A customer banner is 19 lines high and can be up to 80 characters long.

Before you begin

Select **custom** for the ACLI banner type.

Procedure

- 1. In the navigation tree, click **Edit**.
- 2. In the Edit tree, click Chassis.
- 3. In the Chassis tree, click Chassis.
- 4. In the work area, select the **Custom Banner** tab.
- 5. To select a switch for which to customize the banner, click a row.
- 6. In the row, double-click the cell in the **Line** column.
- 7. Type a character string for the banner.
- 8. On the toolbar, click Apply.

Custom Banner tab field descriptions

The following table describes the fields on the Custom Banner tab.

Name	Description
Туре	Indicates whether the banner type is for a standalone (switch) or a stack (stack). Stack is not available for Release 5.0
Id	Indicates the line of text within a custom banner.
Line	Specifies the banner character string. The custom banner is 19 lines high and can be up to 80 characters long.

Changing switch software using EDM

Use this procedure to change the software version running on the switch.

Procedure

- 1. In the navigation tree, click Edit.
- In the Edit tree, click File System.
- 3. On the work area, click the **Config/Image/Diag file** tab.
- 4. In the **TftpServerInetAddressType** section, click a radio button.
- 5. In the **TftpServerInetAddress** dialog box, type the TFTP server IP address.
- 6. In the **BinaryConfigFileName** dialog box, type the name of the binary configuration file.
- 7. In the **ImageFileName** dialog box, type the name of the current image file.
- 8. In the **FwFileName(Diagnostics)** dialog box, type the name of the current diagnostic file.
- 9. In the **Action** section, click a radio button.
- 10. On the toolbar, click **Apply**.

104 Getting Started March 2013

Config Image Diag file tab field descriptions

The following table describes the fields on the Config/Image/Diag file tab.

Name	Description
TftpServerInetAddressType	Specifies the type of TFTP address:
	• IPv4
	• IPv6
TftpServerInetAddress	Specifies the IP address of the TFTP server on which the new software images are stored for download.
BinaryConfigFileName	Specifies the binary configuration file currently associated with the switch.
ImageFileName	Specifies the name of the image file currently associated with the switch. You can change this value to the name of the software image to be downloaded.
FwFileName(Diagnostics)	Specifies the name of the diagnostic file currently associated with the switch. You can change this field to the name of the diagnostic software image to be downloaded.
Action	Specifies the actions taken during this file system operation. The available options are:
	• other
	dnldConfig: downloads a configuration file to the switch. The new configuration file is implemented on the next switch boot cycle.
	upldConfig: uploads a configuration file to a server from the switch. The configuration file contains the current switch MIB object value.
	dnldlmg: downloads a new software image to the switch.
	dnldlmglfNewer: downloads a new software image to the switch only if it is newer than the image currently in use.
	dnldlmgNoReset: downloads a new software image to the switch, but does not

Name	Description
	reset the switch when the download is complete.
	dnldFw: downloads new firmware to the switch.
	dnldFwNoReset: downloads new firmware to the switch, but does not reset the switch when the download is complete.
Status	Displays the status of the last action that occurred since the switch last booted. Values include:
	other: no action occurred since the last boot.
	• inProgress: the selected operation is in progress.
	success: the selected operation succeeded.
	• fail: the selected operation failed.

Viewing the agent and image software load status using EDM

Use this procedure to display the currently loaded and operational software status for agent and image loads for an individual switch.

Procedure

- 1. In the navigation tree, double-click **Edit**.
- 2. In the Edit tree, click File System.
- 3. In the work area, click the **Boot Image** tab to view the software status.

106 Getting Started March 2013

Boot Image tab field descriptions

The following table describes the fields on the Boot Image tab.

Name	Description
Unit # Software Image version	Indicates the loaded agent software image for the switch.
Unit # Software Image in flash	Indicates the operational agent software image for the switch.
Unit # Diag Image version	Indicates the loaded diagnostic software image for the switch.
Unit # Diag Image in flash	Indicates the operational diagnostic software image for the switch.

Configuring SNTP using EDM

Use this procedure to configure Simple Network Time Protocol (SNTP).

Procedure

- 1. In the navigation tree, click **Edit**.
- 2. In the Edit tree, click **SNTP/Clock**.
- 3. In the work area, click the **Simple Network Time Protocol** tab.
- 4. In the **PrimaryServerInetAddressType** section, click a radio button.
- 5. In the **PrimaryServerInetAddress** dialog box, type a value.
- 6. In the **SecondaryServerInetAddressType** section, click a radio button.
- 7. In the **SecondaryServerInetAddress** dialog box, type a value.
- 8. In the **State** section, click a radio button.
- 9. In the **SyncInterval** dialog box, type a value.
- 10. In the **ManualSyncRequest** section, click the **requestSync** radio button to synchronize the switch with the NTP server.
- 11. On the toolbar, click **Apply**.

Simple Network Time Protocol tab field descriptions

The following table describes the fields on the Simple Network Time Protocol tab.

Name	Description
PrimaryServerAddressType	Specifies the primary SNTP server IP address type. Values include ipv4 and ipv6.
PrimaryServerAddress	Specifies the IP address of the primary SNTP server.
SecondaryServerAddressType	Specifies the secondary SNTP server IP address type. Values include ipv4 and ipv6.
SecondaryServerAddress	Specifies the IP address of the secondary SNTP server.
State	Specifies if the switch uses SNTP to synchronize the switch clock to the Coordinated Universal Time (UTC).
	disabled: the device cannot synchronize its clock using SNTP
	enabled (unicast): the device synchronizes to UTC shortly after start time when network access becomes available, and periodically thereafter.
	Important:
	To clear the PrimaryServerAddress and SecondaryServerAddress, you must first set the State to disabled.
SyncInterval	Specifies the frequency, in hours, that the device attempts to synchronize with the SNTP servers. Values range from 0 to 168. With a value of 0, synchronization occurs only when the switch boots up
ManualSyncRequest	Specifies that the device will immediately attempt to synchronize with the SNTP servers.
LastSyncTime	Indicates the Coordinated Universal Time (UTC) when the device last synchronized with an SNTP server. This is a read-only value.
LastSyncSourceInetAddressType	Indicates the IP address type of the SNTP server with which this device last synchronized. This is a read-only value.

Name	Description
LastSyncSourceInetAddress	Indicates the IP address of the SNTP server with which this device last synchronized. This is a read-only value.
NextSyncTime	Indicates the UTC at which the next synchronization is scheduled. This is a readonly value.
PrimaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the primary server address. However, synchronization with the secondary server address can still occur. This is a read-only value.
SecondaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the secondary server address. This is a read-only value.
CurrentTime	Indicates the current switch UTC. This is a read-only value.

Configuring local time zone using EDM

Use this procedure to configure the local time zone for the switch geographical location.

Procedure

- 1. In the navigation tree, click **Edit**.
- 2. In the Edit tree, click SNTP/Clock.
- 3. In the work area, click the **Time Zone** tab.
- 4. In the **TimeZone** box, select the time zone offset.
- 5. In the **TimeZoneAcronym** dialog box, type a time zone acronym.
- 6. On the toolbar, click Apply.

Time Zone tab field descriptions

The following table describes the fields on the Time Zone tab.

Name	Description
TimeZone	Specifies the time zone of the switch, measured as an offset in 15–minute increments from Greenwich Mean Time (GMT).
TimeZoneAcronym	Specifies the time zone acronym.

Configuring daylight savings time using EDM

Use this procedure to configure the start and end of the daylight savings time period.

Before you begin

Disable the summer time recurring feature.

Procedure

- 1. In the navigation tree, click Edit.
- 2. In the Edit tree, click SNTP/Clock.
- 3. In the work area, click the **Daylight Saving Time** tab.
- 4. In the **Offset** dialog box, type a value.
- 5. In the **TimeZoneAcronym**dialog box, type the time zone acronym.
- 6. In the **StartYear** dialog box, type a value.
- 7. In the **StartMonth** box, select a month.
- 8. In the **StartDay** dialog box, type a value.
- 9. In the StartHour box, select an hour.
- 10. In the **StartMinutes** dialog box, type a value.
- 11. Click **Enabled** to enable daylight savings time.
- 12. Click Apply.
- 13. In the **EndYear** dialog box, type a value.
- 14. In the **EndMonth** box, select a month.
- 15. In the **EndDay** dialog box, type a value.

- 16. In the **EndHour** box, select an hour.
- 17. In the **EndMinutes** dialog box, type a value.
- 18. Perform one of the following:
 - Select the **Enabled** check box to enable daylight savings time for the switch.
 - Clear the **Enabled** check box to disable daylight savings time for the switch.
- 19. Click Apply.

Daylight Saving Time tab field descriptions

The following table describes the fields on the Daylight Saving Tlme tab.

Name	Description
Offset	Specifies the time in minutes by which you want to change the time when daylight savings begins and ends. The offset is added to the current time when daylight savings time begins and subtracted from the current time when daylight savings time ends.
TimeZoneAcronym	Specifies a time zone acronym.
StartYear	Specifies the year when you want to start the daylight savings time.
StartMonth	Specifies the month of each year when you want to start the daylight savings time.
StartDay	Specifies the day of the particular month when you want to start the daylight savings time.
StartHour	Specifies the hour of the particular day when you want to start the daylight saving time.
StartMinutes	Specifies the minutes of the particular hour when you want to start the daylight savings time.
EndYear	Specifies the year when you want to end the daylight savings time.
EndMonth	Specifies the month of each year when you want to end daylight savings time.
EndDay	Specifies the day of the particular month when you want to end daylight savings time.

Name	Description
EndHour	Specifies the hour of the particular day when you want to end daylight savings time.
EndMinutes	Specifies the minute of the particular hour when you want to end daylight savings time.
Enabled	Enables or disables daylight savings time.
	Important:
	Before you enable daylight savings time, configure the feature attributes.

Configuring recurring daylight saving time using EDM

Use this procedure to configure the daylight saving time start and end times for a single occurrence or to recur yearly.

Procedure

- 1. In the navigation tree, click **Edit**.
- 2. In the Edit tree, click SNTP/Clock.
- 3. In the work area, click the **SummerTimeRecurring** tab.
- 4. Perform one of the following:
 - Select the Recurring check box to enable recurring daylight savings time for the switch OR
 - Clear the Recurring check box to disable recurring daylight savings time for the switch.
- 5. In the **RecurringStartMonth** section, click a radio button.
- 6. In the RecurringStartWeek dialog box, type a value.
- 7. In the **RecurringStartDay** section, click a radio button.
- 8. In the **RecurringStartHour** dialog box, type a value.
- 9. In the **RecurringStartMinute** dialog box, type a value.
- 10. In the **RecurringEndMonth** section, click a radio button.
- 11. In the **RecurringEndWeek** dialog box, type a value.
- 12. In the **RecurringEndDay** section, click a radio button.
- 13. In the **RecurringEndHour** dialog box, type a value

- 14. In the **RecurringEndMinute** dialog box, type a value.
- 15. In the **RecurringOffset** dialog box, type a value.
- 16. On the toolbar, click Apply.

SummerTimeRecurring tab field descriptions

The following table describes the fields on the SummerTimeRecurring tab.

Name	Description
Recurring	When selected, enables daylight savings time to recur yearly.
RecurringStartMonth	Specifies the month of each year you want recurring daylight savings time to start.
RecurringStartWeek	Specifies the week of the month you want recurring daylight savings time to start.
RecurringStartHour	Specifies the hour of the particular day you want recurring daylight savings time to start.
RecurringStartMinute	Specifies the minutes of the particular hour you want recurring daylight savings time to start.
RecurringEndMonth	Specifies the month of each year you want recurring daylight savings time to end.
RecurringEndWeek	Specifies the week of the month you want recurring daylight savings time to end.
RecurringEndDay	Specifies the day of the particular month you want recurring daylight savings time to end.
RecurringEndHour	Specifies the hour of the particular day you want recurring daylight savings time to end.
RecurringEndMinute	Specifies the minutes of the particular hour you want recurring daylight savings time to end.
RecurringOffset	Specifies the time in minutes by which you want to change the time when recurring daylight savings begins and ends. The offset is added to the current time when daylight savings time begins and subtracted from the current time when daylight savings time ends.

Configuring the switch using EDM

Chapter 14: Managing Power over Ethernet (PoE) using EDM

Managing switch PoE using EDM

Use this procedure to display and manage Power over Ethernet (PoE) for a switch unit.

Procedure

- 1. From the Device Physical View, click a switch unit with PoE ports.
- 2. From the navigation tree, click Edit.
- 3. In the Edit tree, click Unit.
- 4. In the work area, click the **PoE** tab.
- 5. In the **UsageThreshold%**, type a value.
- 6. Perform one of the following:
 - To enable the sending of traps if the switch power usage exceeds the configured threshold percentage, select the NotificationControlEnable check box.

OR

- To disable the sending of traps if the switch power usage exceeds the configured threshold percentage, clear the NotificationControlEnable check box.
- 7. In the **PoweredDeviceDetectType** section, click a radio button.
- 8. On the toolbar, click **Apply**.

PoE tab field descriptions

The following table describes the fields on the PoE tab.

Name	Description
Power(watts)	Displays the total power (in watts) available to the switch.
OperStatus	Displays the power state of the switch:
	• on
	• off
	• faulty
ConsumptionPower(watts)	Displays the power (in watts) being used by the switch.
UsageThreshold%	Lets you set a percentage of the total power usage of the switch above which the system sends a trap.
	• Important:
	You must enable the traps (NotificationControlEnable) to receive a power usage trap.
NotificationControlEnable	Lets you enable or disable sending traps if the switch power usage exceeds the percentage set in the UsageThreshold% field.
PoweredDeviceDetectType	Lets you set the power detection type that the switch uses to detect a request for power from a device connected to all ports on the switch:
	• 802.3af
	802.3af and legacy support
	• 802.3at
	802.3at and legacy support
	Important:
	The default setting is 802.3af. Ensure that this setting matches the setting for the detection type used by the powered devices on this switch.

Name	Description
PowerPresent	Specifies the currently used power source. Available power sources are AC and DC. A value of acOnly indicates that the only power supply is AC. A value of dcOnly indicates that the only power supply is DC. A values of acDc indicates that there are two power supplies; both AC and DC are supplying power.

Viewing PoE information for switch ports using EDM

Use this procedure to display the PoE configuration for switch ports.

Procedure

- 1. In the navigation tree, click **Edit**.
- 2. In the Edit tree, click Chassis.
- 3. Click Ports.
- 4. In the work area, click the **PoE** tab.

PoE tab field descriptions

The following table describes the fields on the PoE tab.

Name	Description
AdminEnable	Lets you enable or disable PoE on this port. By default, PoE is enabled.
DetectionStatus	Displays the operational status of the power-device detecting mode on the specified port:
	disabled: detecting function disabled.
	searching: detecting function is enabled and the system is searching for a valid powered device on this port.
	deliveringPower: detection found a valid powered device and the port is delivering power.
	• fault: power-specific fault detected on port

Name	Description
	• test: detecting device in test mode.
	otherFault
	Important: Avaya recommends against using the test
	operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Lets you set the power priority for the specified port to:
	• critical
	• high
	• low
PowerLimit(watts)	Specifies the maximum power that the switch can supply to a port. RANGE: 3 to 32 Watts DEFAULT: 16 Watts
Voltage (volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

Configuring PoE power mode using EDM

The ERS 3510GT-PWR+ switch is able to operate in two Power over Ethernet (PoE) budget modes:

- Fanless mode Low Power Mode
- Normal mode High Power Mode

The default is: High Power Mode (Normal mode).

In Fanless mode, the fan is shut down and will not be activated, despite the internal temperature. To prevent the switch from overheating, the PoE budget is limited to 60 Watts. Although the internal temperature may show as High in this mode, the ERS 3510GT-PWR+

switch has been designed to operate at internal temperatures above 60°C. When the switch is operating in Fanless mode, diagnostic fan tests are not performed.

In Normal mode, the fan operates normally and is activated when the temperature reaches its threshold. See <u>Managing switch PoE using EDM</u> on page 115. In Normal mode, the PoE budget is not limited; a maximum of 170 Watts is available.

Use this procedure to set the PoE power mode.

Procedure

- 1. In the navigation tree, double-click **Power Management** .
- 2. Click PoE.
- 3. In the work area, click the **Power Mode** tab.
- 4. Perform one of the following:
 - To enable Low Power Mode and disable fan operation, select the **lowPowerBudget** checkbox.

OR

- To enable High Power Mode and enable fan operation, select the **highPowerBudget** checkbox.
- 5. On the toolbar, click Apply.

Power Mode tab field descriptions

The following table describes the fields on Power Mode tab.

Name	Description
PoEPowerMode	Lets you set the power mode for switch to be either:
	lowPowerBudget: Sets the switch PoE budget to 60W max and disables fan operation (Fanless mode).
	highPowerBudget: Sets the switch PoE budget to 170W max and enables fan operation (Normal mode).
	DEFAULT: highPowerBudget (Normal mode)

Managing Power over Ethernet (PoE) using EDM