Avaya Ethernet Routing Switch 3500 Series Getting Started

Release 5.1
NN47203-301
Issue 02.02
February 2013

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya 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.

Contents

Chapter 1: Purpose of this document

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

Chapter 2: New in this release

The following hardware and software features are new in Avaya Ethernet Routing Switch (ERS) 3500 Series Release 5.1:

ERS 3500 hardware

The following table lists and describes the new stack cables that are supported in Release 5.1:

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

ERS 3500 software features

The following software features are new for ERS 3500 Series Release 5.1:

- 802.1X EAP Separate enable/disable
- 802.1X EAP and NEAP accounting
- Agent Auto Unit Replacement (AAUR)
- Auto Unit Replacement (AUR)
- DHCP Server
- Diagnostics Auto Unit Replacement (DAUR)
- Distributed LAG (802.3ad LACP)
- Distributed MLT
- Identify Units (Blink LEDs)
- LLDP configurable MED network policy (5.0.1)
- Run IP Office Script (5.0.1)
- SLAMon Agent (5.0.2)
- Show UTC Timestamp (5.0.2)
- Stack Forced Mode (for 2 unit stacks)
- Stack Health Check
- Stack IP address
- Stack Monitor and Statistics

- Storm Control
- Unit Stack uptime
- Voice VLAN Integration (5.0.1)

Features

See the following sections for information about feature-related changes.

Agent Auto Unit Replacement (AAUR)

As part of Auto Unit Replacement functionality, Agent Auto Unit Replacement (AAUR), is used to ensure that all units in a stack have the same software image by inspecting units joining a stack and downloading the stack software agent image to any unit that has a dissimilar image. AAUR is enabled by default.

For more information, see

- Agent Auto Unit Replacement (AAUR) on page 34
- AAUR configuration on page 89

Auto Unit Replacement (AUR)

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

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

For more information, see

- Auto Unit Replacement (AUR) on page 27
- AUR configuration on page 86

Diagnostics Auto Unit Replacement (DAUR)

As part of Auto Unit Replacement functionality, Diagnostic Auto Unit Replacement (DAUR) is used to update the diagnostic image on a non-base unit with the diagnostic image saved in the base unit of a switch stack, if the images differ. When you enable or disable Agent Auto Unit Replacement (AAUR), you automatically enable or disable DAUR in conjunction with AAUR. The default setting for AAUR and DAUR is enabled.

For more information, see Diagnostics Auto Unit Replacement (DAUR) on page 35.

Identify Units (Blink LEDs)

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

Following a reset or power up, if the switch detects power on its stacking cables and is connected to another unit, the switch shuts down all its local ports. When the ports are disabled,

the port LEDs blink, similar to ports that are shut down. The ports are reenabled when the unit finishes entering the stack formation or after a 60–second timeout, whichever comes first.

If the unit does not detect power on the stacking ports in 30 seconds after it comes up, ports forward the traffic.

For more information, see Configuring LEDs to blink on the display panel on page 68.

Run IP Office Script (5.0.1)

This feature introduces an ACLI script that configures parameters for the ERS 3500 switch according to Avaya best practices for converged solutions. The script can be executed in automatic mode where the configuration set with pre-determined parameters or in verbose mode where the installer can enter parameters when prompted by ACLI. The script configuration setup is optimized for solutions with IP Office supporting approximately 2 to 22 users, so that a technician can quickly and easily set up an ERS 3500 switch in a best practices solution with Avaya IP Office. In Release 5.1 with stacking support, the script can now support up to 192 switch ports. The script sets VLAN IDs, IP addresses, QoS rules and tagging modes on switch ports to specific values and PoE priorities for PWR units. LLDP for IP Phone detection is set automatically and switch ports are configured to which the IP Office call server can connect. The script executes the set of CLI commands using the ACLI command **`run ipoffice`** (fully automated configuration), or **`run ipoffice verbose`** (user prompted configuration). The script settings can be displayed using the **`show running-config`** command. The script is available in both standalone and stacking mode. In stacking mode, you must execute the script from the Base Unit.

For more information, see IP Office Script on page 56.

Show UTC Timestamp

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

For more information, see Enabling or disabling UTC timestamp in CLI show command outputs ACLI on page 81.

Stack Forced Mode

Stack Forced Mode primarily provides management IP continuity of a two-unit stack if one unit fails in the stack. This extends to a two-unit stack that may both become stand-alone switches if the stacking mechanism between both units fails. You can manage the units from the broken stack in Stack Forced Mode, depending on the location of uplink(s). If you enable Stack Forced Mode on a stack, you enable Stack Forced Mode on both units in the two-unit stack. Stack Forced Mode becomes active only if the stack fails.

For more information, see Stack forced mode on page 24.

Stack IP Address

You can assign an IP Address to the base unit switch in a switch stack using ACLI.

For more information, see Setting the IP address on page 41.

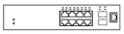
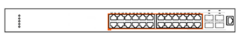
Chapter 3: Getting started fundamentals

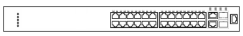
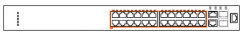
Introduction to ERS 3500 switch models

There are six different Ethernet Routing Switch 3500 Series models as described in the table below.

Note:

All switch models support autopolarity.

Front View	Model	Part Number	Description
	ERS 3510GT	AL3500?14–E6	8 10/100/1000BaseT ports, plus two SFP ports (ports 9 and 10). Standalone and fanless.
	ERS 3510GT-PWR+	AL3500?14–E6	8 10/100/1000BaseT PoE+ ports (802.3af/at), plus two SFP ports (ports 9 and 10). Standalone. Fanless operation in Low Power Budget mode @ 60W max PoE budget, or normal fan operation in High Power Budget mode @ 170W max PoE budget.
	ERS 3524GT	AL3500?05–E6	24 10/100/1000BaseT ports, four SFP ports shared with ports 21–24, plus two SFP rear ports. Stackable
	ERS 3524GT-PWR+	AL3500?15–E6	24 10/100/1000BaseT PoE+ ports (802.3af/

Front View	Model	Part Number	Description
			at), four SFP ports shared with ports 21–24, plus two SFP rear ports. Stackable
	ERS 3526T	AL3500?01–E6	24 10/100BaseT ports, plus two 10/100/1000 or Small Form Pluggable (SFP) front combination ports, plus two SFP rear ports. Fanless. Stackable
	ERS 3526T-PWR+	AL3500?11–E6	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. Stackable

Question marks (?) in the table above 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

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 ifconfig 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`

Command mode and sample prompt	Entrance commands	Exit commands
Privileged Executive 3526T#	enable	exit or logout
Global Configuration 3526T<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>#	From Global Configuration mode: To configure a port enter interface fastethernet <port number> To configure a VLAN enter interface vlan <vlan number>	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, IPv6 default gateway and DHCP server.

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
- IPV6 address/prefix
- IPV6 default gateway
- DHCP server information (optional)

Before you begin

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

Procedure

1. Press
   `CTRL + Y` to obtain a CLI prompt.
2. Enter **`enable`**
3. 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 [192.168.10.6]:`
5. Enter the default gateway IP address at the following prompt:
   `Please provide the Default Gateway [0.0.0.0]:`
6. Enter the read only community string at the following prompt:
   `Please provide the Read-Only Community String [**********]:`
7. Enter the read write community string at the following prompt:
   `Please provide the Read-Write Community String [**********]:`
8. Enter the VLAN ID for the Quick Start at the following prompt:
   `Please provide the Quick Start VLAN <1–4094> [1]:`
9. Enter the in-band IPv6 address at the following prompt:
   `Please provide the in-band IPV6 Address/Prefix_length [ : :/0]:`
10. Enter the in-band IPv6 default gateway at the following prompt:
    `Please provide the in-band IPV6 Default Gateway [ : :]:`
11. At the “Do you want to enable the DHCP server? prompt, enter `Y` to enable the DHCP server, OR leave the prompt at `N` if you do not want to enable the DHCP server.

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

Example

```
################################################################################
         Welcome to the ERS3500 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[192.168.10.6]:
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[::]:
Do you want to enable the DHCP server? y/n [n]:


################################################################################
Basic stack 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.
- When a stack is booted, the default IP address is 192.168.1.2 instead of 192.186.1.1 when in standalone.

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 in-band 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, stack, or each unit within a stack. An Asset ID consists of an alphanumeric string of up to 32 characters in length for the switch or stack. 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 or stack 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 [stack | unit <1–8>] <WORD>
   ```
3. Verify the Asset ID using one of the following commands:
   ```
   show system
   ```
   OR
   ```
   show tech
   ```
   OR

```
show sys-info
```

OR

```
show running-config module asset-id
```

Variable definitions

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

Variable	Value
stack	Configures the Asset ID of a stack.
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.

Stack forced mode

Stack Forced Mode allows one or both units of a two-unit stack to become stand-alone switches if a stack of two units fails. You can manage the units from the broken stack in Stack Forced Mode.

If you enable Stack Forced Mode on a stack, you enable Stack Forced Mode on both units in the stack. Stack Forced Mode becomes active only if the stack fails.

You can configure Stack Forced Mode through ACLI. Refer to Enabling or disabling stack forced mode on page 83.

Stack Forced Mode applies to a stand-alone switch that is part of a stack of two units. When functioning in this mode, the stand-alone switch keeps the previous stack IP settings (IP address, netmask, and gateway). An administrator can reach the device through an IP connection by Telnet or Enterprise Device Manager while using Stack Forced Mode.

If one unit fails, the remaining unit (base or non-base unit) keeps the previous stack IP settings. The remaining unit issues a gratuitous ARP packet when it enters Stack Forced Mode, in order for other devices on the network to update their ARP cache.

If the stack connection between the two units fails (a stack cable failure, for example), both stand-alone units retain the IP settings. To detect if the other stack partner is also using the previous stack IP settings, each device issues an ARP request on the IP address.

Non-EAP clients connected to the device can still authenticate themselves and maintain connectivity to the network using Stack Forced Mode. Non-EAP clients authenticate by the device with RADIUS, which is based on the stack IP address. In Stack Forced Mode, the device retains the IP settings of the stack of two.

The functional unit stays in Stack Forced Mode until either a reboot or it joins a stack.

A settlement timer prevents several stack failures that occur at an interval of a few seconds to lead to a device entering Stack Forced Mode after it was part of a stack larger than two units. A device enters Stack Forced Mode if and only if it was part of a stack of two for 30 seconds or longer.

Stacking fundamentals

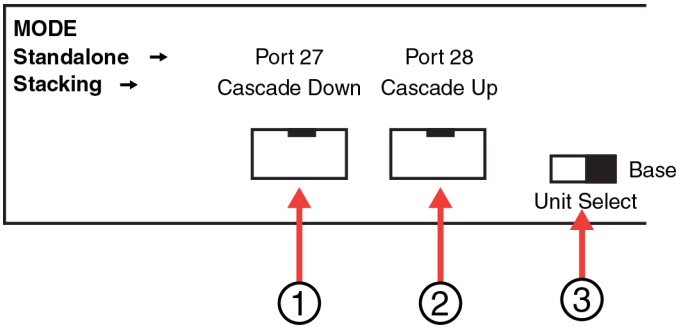
This section contains information about the stacking features, such as stack capabilities, stacking functionality delivery, stack configurations, and Auto Unit Replacement.

Stacking capabilities

The following Avaya Ethernet Routing Switch 3500 Series units support stacking capability in Release 5.1: ERS 3524GT, ERS 3524GT-PWR+, ERS 3526T, and ERS 3526T-PWR+. The two rear ports on these models can be used in either Standalone Mode (default) or Stacking Mode.

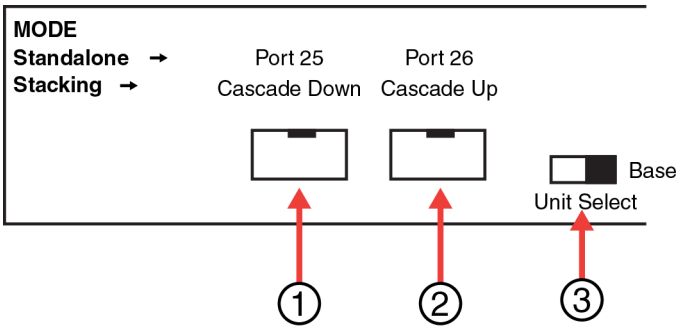
- **Standalone Mode —** In this mode, the ERS 3500 switch rear ports function as follows:
  - Provides two additional uplinks or connections to servers or power users and supports regular port configuration parameters such as Spanning Tree, EAP, VLAN Tagging, MLT/DMLT/VLACP, and port enable/disable
  - Provides fixed port speed at 1000 Mbps Full Duplex operation with the insertion of a supported SFP in the rear ports. Link and traffic indications are provided on the front left of each switch where the LEDs for the rear ports illustrate “Down / 27” and “Up / 28” for the ERS 3526T models, and “Down / 25” and “Up / 26” on the ERS 3524GT models, as shown in the figures that follow.
- **Stacking Mode** — In this mode, the ERS 3500 switch rear ports function as follows:

- Provides resilient stacking of up to eight units (ERS 3526T, ERS 3526T-PWR+, ERS 3524GT , and ERS 3524GT-PWR+ switches only) when the two rear SFP ports are configured for “Stacking Mode” operation
- LEDs on the front panel of the switches indicate “Base Unit” selection and rear stack port Up/Down connection status.
- Rear ports operate at 10 Gbps bandwidth for an aggregate of up to 80 Gbps for a stack of eight units.



1 = Cascade down port
2 = Cascade up port
3 = Base Unit Select Switch - used to designate the Base Unit in a stack. When set to the RIGHT position, this unit acts as the Base Unit for the stack

Figure 1: ERS 3526T and ERS 3526T-PWR+ rear ports



1 = Cascade down port
2 = Cascade up port
3 = Base Unit Select Switch - used to designate the Base Unit in a stack. When set to the RIGHT position, this unit acts as the Base Unit for the stack

Figure 2: ERS 3524GT and ERS 3524GT-PWR+ rear ports

For more information on stacking, refer to the following:

- The correct Avaya SFP direct attach cable is required in order to enable and use Stacking Mode. Stacking cables must be ordered separately (refer to New in this release on page 11 for more information on stacking cable order codes and lengths).
- For information on how to configure stacking, refer to *Avaya Ethernet Routing Switch 3500 Series — Regulatory Information Guide* , (NN47203–100).
- For stacking procedures using ACLI, refer to Configuring the operational mode on rear ports on page 85.
- For stacking procedures using EDM, refer to Rear ports mode configuration on page 146.

Auto Unit Replacement (AUR)

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

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

Important:

In order for AUR to function properly, the new unit and the existing units in the stack must all be running the same version of software. If that is not the case, it must have at least release 5.1 software, so that image can be updated using AAUR feature.

Important:

AUR is intended for a stack configuration of two or more units. In a two-unit stack configuration, if a unit fails, the remaining unit becomes a stand-alone switch. AUR loads the configuration of the failed unit in the replacement of ERS 3500 Series unit only if the failed unit was a non-Base Unit.

Other information related to this feature:

- The new unit must be the same hardware configuration as the old, including the same number of ports.
- If the administrator adds a new unit with a different hardware configuration, the configuration of this unit is used.
- If the administrator adds a new unit with the same hardware configuration, the previous configuration of the new unit is lost. The previous configuration of the new unit is overwritten with the restored configuration from the stack.

- This feature can be disabled/enabled at any time with ACLI. The default mode is ENABLE.
- Customer log messages are provided.

Important:

After starting a stack, use ACLI command **`show stack auto-unit-replacement`** from a unit console to find out if that unit is ready for replacement.

AUR function

The CFG mirror image is a mirror of a CFG image (in FLASH) of a unit in a stack. The mirror image does not reside in the same unit with the CFG image. The unit that contains the CFG image is called the Associated Unit (AU) of the CFG mirror image. The MAC Address of the AU is called the Associated Mac Address (AMA) of the CFG mirror image.

An active CFG Mirror Image is a CFG mirror image that has its AU in the stack. An INACTIVE CFG Mirror Image is a CFG mirror image for which the associated AU has been removed from the stack. When a CFG mirror image becomes INACTIVE, the INACTIVE CFG mirror image is copied to another unit.

The stack always keeps two copies of an INACTIVE CFG mirror image in the stack in case one unit is removed-the other unit can still provide the backup INACTIVE CFG mirror image.

CFG mirror image process

The CFG mirror image process is triggered by specific events.

Power Cycle:

After a power cycle, all the CFG images in a stack are mirrored.

The figure that follows illustrates the CFG mirror images in a three-unit stack after the stack is powered on. Unit 1 is the Based Unit (BU) and all other units are Non-Based Units (NBU).

- Unit 1 (BU) contains mirror images for unit 2 (CFG 2) and unit 3 (CFG 3).
- Unit 2 (NBU), is the TEMP-BU. It contains a mirror image of unit 1 (CFG 1), in case the BU (unit 1) is removed from the stack.
- All three mirror images (CFG 1, CFG 2, and CFG 3) are active.
- Unit 2 is the Associated Unit of the CFG 2 mirror image.
- The MAC Address 2 is the Associated MAC Address (AMA) of the CFG 2 mirror image.

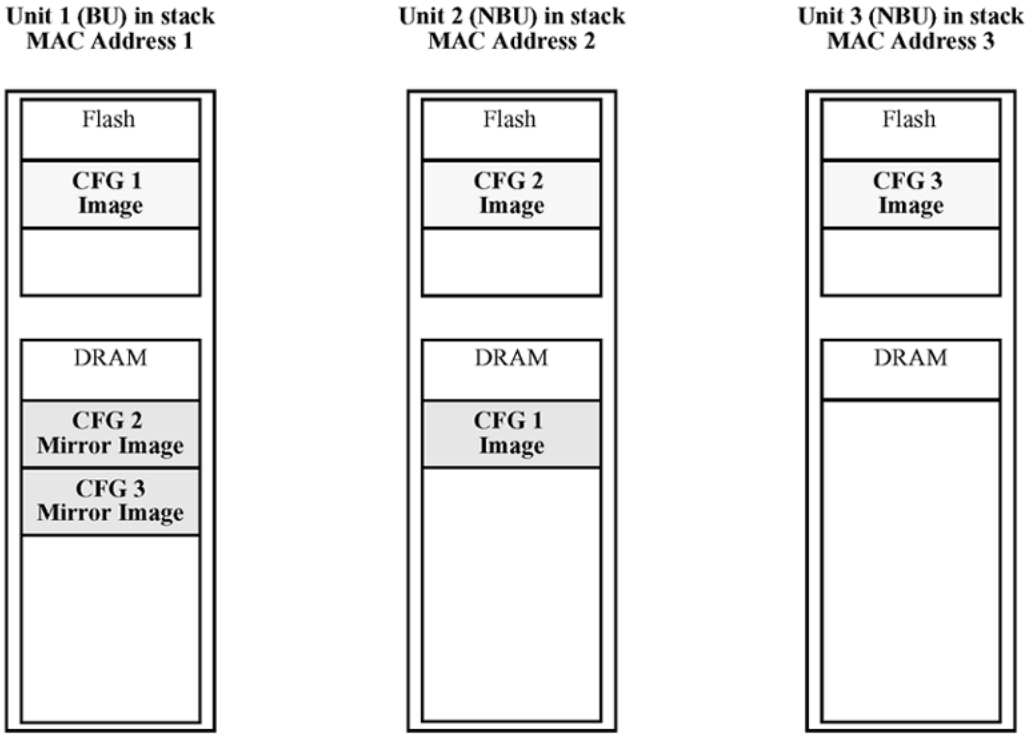


Figure 3: CFG mirror process in stack

Adding a unit:

In a stack that does not have any INACTIVE CFG mirror images, adding a new unit causes the CFG image of the new unit to be mirrored in the stack. For example, in the figure that follows, after adding unit 4 to the stack, the CFG 4 mirror image is created in the BU (unit 1).

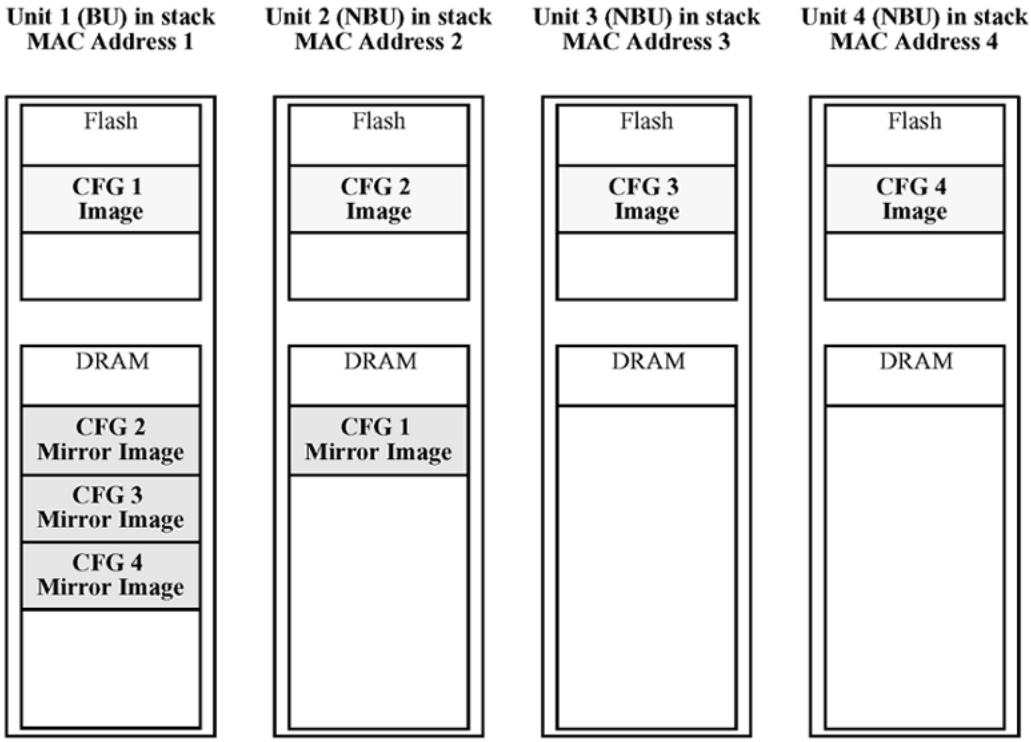


Figure 4: CFG mirror images in the stack after adding unit 4

Removing an NBU:

When an NBU is removed from a stack, the related CFG mirror image in the stack becomes INACTIVE.

The AUR feature ensures that the stack always has two copies of an INACTIVE CFG mirror image. These two copies must not reside in the same unit in the stack.

For example, after the removal of unit 4 from the stack, the CFG 4 mirror image becomes INACTIVE (shown in the figure that follows). Another copy of the INACTIVE CFG 4 mirror image is also created in unit 2.

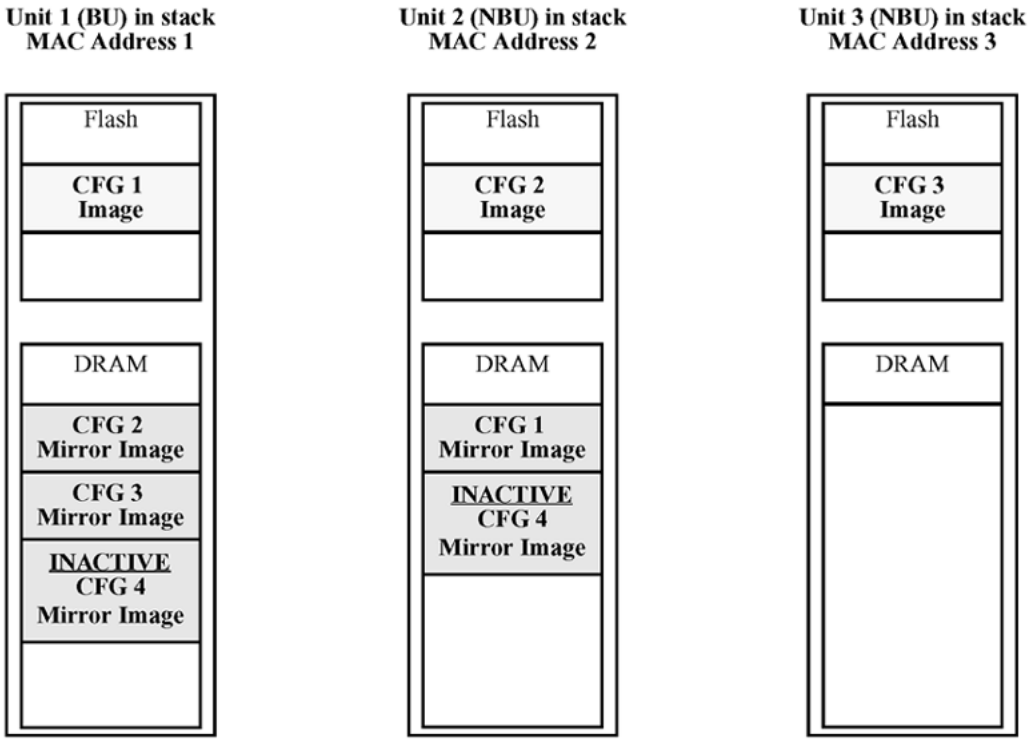


Figure 5: CFG mirror images after removing unit 4

Removing a BU:

When a BU is removed, the TEMP-BU assumes the role of the BU. Because all the CFG mirror images of the NBUs reside in the removed BU, the TEMP-BU mirrors all the CFG image of the NBUs in the stack.

After the removal of the BU from the stack, the TEMP-BU (unit 2) has to mirror all the CFG images in the stack (as shown in the figure that follows). The feature also ensures that the stack always has two copies of an INACTIVE CFG mirror image.

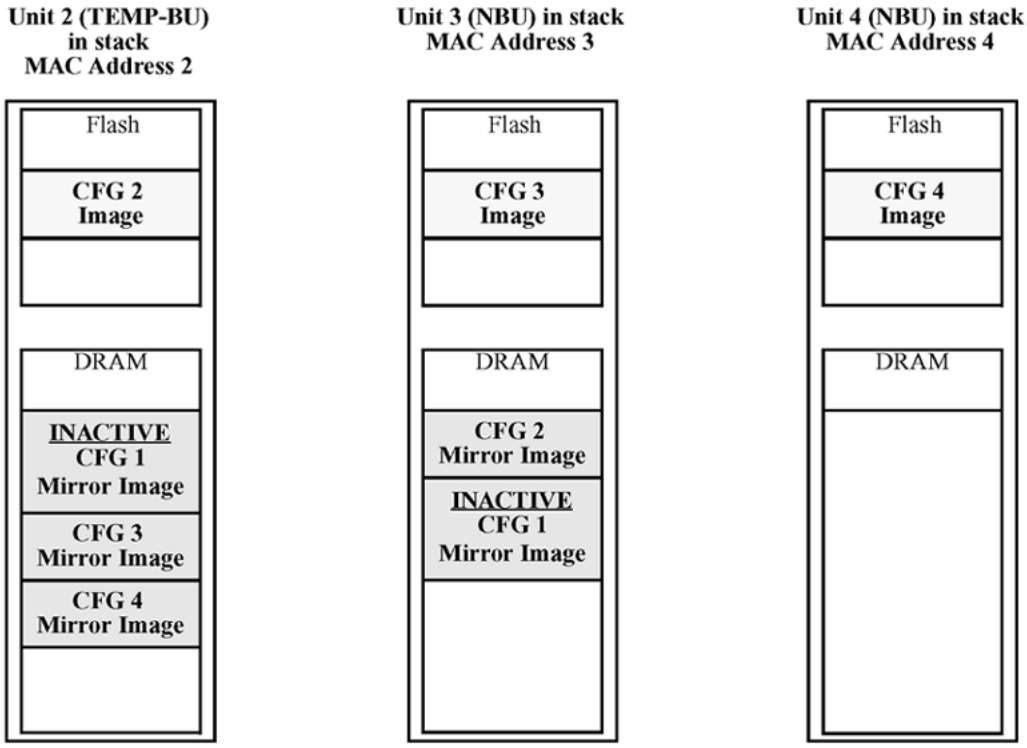


Figure 6: CFG mirror images in the stack after removing the BU (unit 1)

As shown in the previous figure:

- Unit 2 becomes the TEMP-BU.
- The CFG 1 mirror image (residing in unit 2) becomes INACTIVE.
- A second copy of the INACTIVE CFG 1 mirror image is created in unit 3.
- The TEMP-BU (unit 2) contains all CFG mirror images of the stack's NBUs.
- The CFG 2 mirror image is created in unit 3. Unit 3 becomes the next TEMP-BU in case the current TEMP-BU is removed.

Note:

If you have a system of two units or stacks of 3 to 8 units that are in BOTH DIRECTIONS configuration, the CFG of the Base Unit is not mirrored and the Base Unit is not ready for replacement. The CFG for the Base Unit is always mirrored on the next Base Unit (i.e. the unit that becomes the TEMP-BU when the Base Unit fails). In these specific stack configurations, there is no next Base Unit — if the Base Unit fails, the remaining units become standalone.

Restoring a CFG image

Restoring a CFG image is a process that overwrites the CFG image of a new unit in a stack with an INACTIVE mirror image stored in the stack.

Important:

Restore a CFG image to a new unit happens only if the following conditions are met.

- The AUR feature is enabled.
- The MAC Address of the new unit is different from the AMA of the INACTIVE CFG mirror image corresponding to the replaced unit.

The image restore process consists of the following steps:

1. Adding a new unit to a stack
2. The INACTIVE CFG mirror image in the stack is sent to the new unit. The INACTIVE CFG mirror image becomes ACTIVE.
3. The new unit saves the received CFG image to its flash.
4. The new unit resets itself.

For example, if a unit 5 (MAC Address 5) is added to the stack, the following occurs (see the figure that follows):

- The INACTIVE CFG 1 mirror image is copied to the CFG 5 image. Unit 5 now has the configuration of unit 1 that is no longer in the stack.
- The INACTIVE CFG 1 mirror image in unit 2 becomes ACTIVE.
- The INACTIVE CFG 1 mirror image in unit 3 is removed.
- The MAC Address 5 of the unit 5 becomes the new AMA of the CFG 1 mirror image.

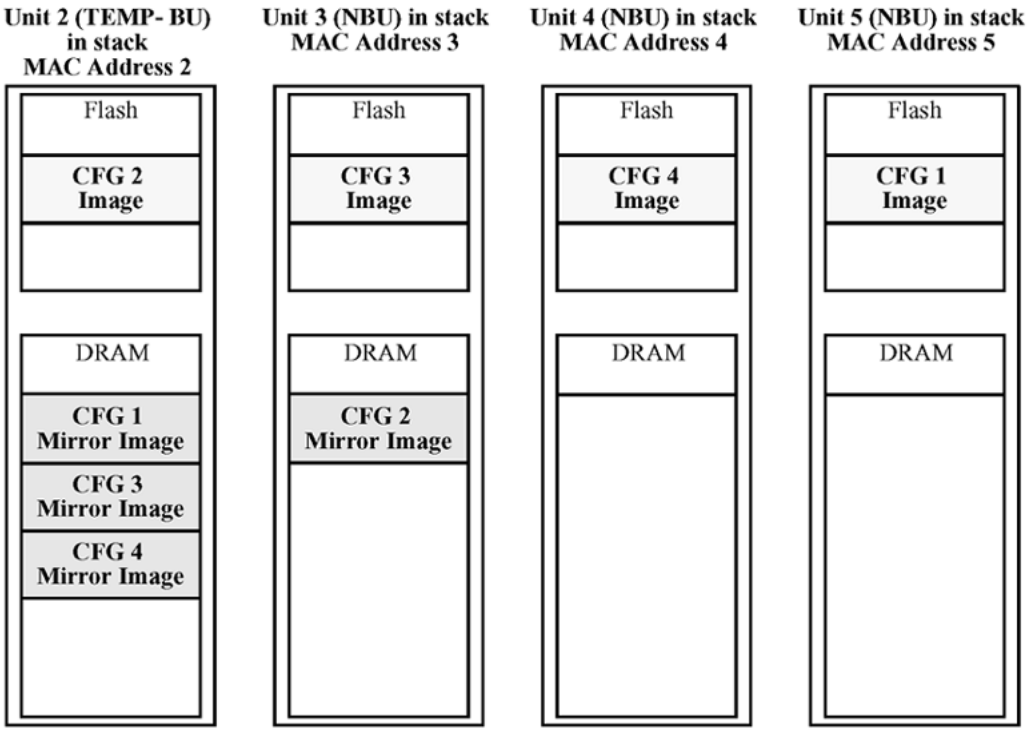


Figure 7: CFG mirror images in the stack after adding unit 5

Synchronizing the CFG mirror images with CFG images

A CFG mirror image is updated whenever a CFG flash synchronization occurs in the AU.

Agent Auto Unit Replacement (AAUR)

Use the enhancement to the Auto Unit Replacement functionality, known as the Agent Auto Unit Replacement (AAUR), to ensure that all units in a stack have the same software image by inspecting units joining a stack and downloading the stack software image to any unit that has a dissimilar image. AAUR is enabled by default.

Agent Auto Unit Replacement functions in the following manner:

1. When a stand-alone switch joins an AAUR-enabled stack, the switch software image is inspected.
2. If the switch software image differs from the stack software image, the AAUR functionality downloads the stack software image to the joining unit.
3. The joining unit is then reset and becomes a member of the stack upon a restart.

Important:

In order for AAUR to function properly, the new unit must be running release 5.1software (or later).

Diagnostics Auto Unit Replacement (DAUR)

In Release 5.1 and up, DAUR is part of the Auto Unit Replacement process, which includes Agent Auto Unit Replacement (AAUR).

When you enable or disable AAUR, you also enable or disable DAUR concurrently. There are no commands to separately enable or disable DAUR.

The default configuration for AAUR is enabled, so DAUR is also enabled by default.

After you enable AAUR, DAUR can update the diagnostic image of the non-base unit with the diagnostic image saved in the base unit of a stack.

DAUR updates the diagnostic image on inserted units in the same way that AAUR performs this function for agent code.

The DAUR process works in conjunction with AAUR. When you insert a new unit into an existing stack, the system checks the diagnostics image against other units and upgrades the diagnostics image of the new unit if necessary.

Release 5.1 and up support DAUR. Previous software releases do not support DAUR. For example, you cannot insert a switch that uses software release 5.0 into an existing stack.

You must meet the following conditions before you connect the stack ports of a replacement unit into a stack. The replacement unit must have:

- a minimum of software release 5.1 loaded
- the rear ports configured and operating in Stacking Mode (the default mode for a stack-enabled switch)

Adding or replacing a stack non-base unit:

When you enable AAUR on a stack and then add another unit with a different software image, this unit does not join the stack immediately. The unit remains in stand-alone mode.

The new unit sends an AAUR request to the up stream port. If the unit does not receive an answer, it sends a request to the downstream port. After the image transfers successfully, the switch reboots.

The log file displays the following messages when DAUR completes successfully:

```
I 2 00:02:01:20 18 DAUR - Info: Receive request for diagnostic image, start transfer
I 2 00:02:01:22 19 DAUR - Info: Diagnostic transfer finished
```

If you add a non-base unit (the base unit select switch is set to off) to an existing operational stack, the non-base unit receives the diagnostic image from the base unit.

When the switch finishes the diagnostic image version update, the switch performs an AAUR check.

Results of the AAUR check:

- If the new unit has the same agent image as the stack, the unit reboots
- If the new unit has a different agent image, the switch performs an AAUR operation

Note:

The new unit added to a stack must have an agent image with software release 5.1 or higher or AAUR and DAUR cannot upgrade the new unit.

The following stacking basics apply:

- If there is more than one unit in a stack with the base selection switch set to base, the unit discovery process fails
- If no units in a stack have the base selection switch set to base, the unit discovery process fails.

After a stack of more than two switches forms, if the base unit stops communicating the system selects a non-base unit as the temporary base unit (TBU). The unit select switch on the TBU is not set to base but the TBU retains its status as base unit, even if the former base unit reboots, until you reboot the stack. The former base unit acts as a non base unit until you reboot the stack.

Replacing a stack base unit:

In a stack of more than two switches, if the base unit fails and the system selects a non-base unit as TBU, when you replace the base unit you must set its base unit selector switch to on. Otherwise, after you power the TBU off, there is no designated base unit and the stack cannot form. The TBU remains as base unit only until it is powered off.

After you replace the base unit, with its base unit selector switch set to on, and all DAUR/AAUR/AUR processes have completed, you can reboot the stack so the new unit becomes the Base Unit. If the stack reboots before all DAUR/AAUR/AUR processes have completed, the stack copies the agent image and diagnostic image of the new unit and the configuration is lost or altered.

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 as shown below.

```
##############################################################################
         Welcome to the ERS3500 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[192.168.1.1]:
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[::]:
Do you want to enable the DHCP server? y/n [n]:


##############################################################################
Basic stack parameters have now been configured and saved.

##############################################################################
```

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

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 or stack. You can also use this procedure to select the boot mode for the next switch reboot.

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.

Note:

If you do not specify the stack or switch parameter, the system automatically modifies the stack IP address when in stack mode and modifies the switch IP address when in standalone mode.

Procedure

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

```
ip address [switch|stack|unit<1–8>][<A.B.C.D>] [netmask
<A.B.C.D>] [default-gateway <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.XXX.XXX; netmask is optional.

Variable	Value
switch | stack | unit <1–8>	Specifies whether to set the IP address for the switch, the stack, or another unit in a stack.
netmask	Sets the IP subnet mask.
default-gateway <*A.B.C.D*>	Sets the IP address of the default gateway.

Clearing the IP address

Use this procedure to clear the existing IP address and subnet mask for the switch or stack or another unit of a stack.

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:
   ```
   no ip address [switch|stack|unit<1–8>]
   ```

Setting the IP address to the default value

Use this procedure to return the IP address of the switch to the default value.

The default value for the switch is 192.168.1.1 for Standalone Mode or 192.168.1.2 for Stacking Mode.

Procedure

1. Log on to the ACLI Global Configuration mode.
2. At the command prompt, enter the following command:
   ```
   default ip address
   ```

Changing subnet netmask value

The subnet mask is set using procedure Setting the IP address on page 41. 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 <A.B.C.D>
```

Variable definitions

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

Variable	Value
<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. **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 or stack or unit 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 | stack | unit <1–8>]][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.

```
3524GT-PWR+(config)#show ip
Bootp/DHCP Mode: BootP Or Default IP

                     Configured           In Use      Last BootP/DHCP
                     -------------    -------------   ---------------
Stack IP Address:    172.16.120.10                    0.0.0.0
Switch IP Address:   172.16.120.12    172.16.120.12   0.0.0.0
Switch Subnet Mask:  255.255.255.0    255.255.255.0   0.0.0.0
Default Gateway:     172.16.120.1     172.16.120.1    0.0.0.0
3524GT-PWR+(config)#
```

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 | stack | unit <1–8>	Specifies the current IP address of the switch or stack or specified unit.
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
                    -------------      -------------    ---------------
Stack IP Address:    172.16.120.10                          0.0.0.0
Switch IP Address:   172.16.120.12     172.16.120.12        0.0.0.0
Switch Subnet Mask:  255.255.255.0     255.255.255.0        0.0.0.0
3524GT-PWR+(config)#
```

Note:

The Router and DNS IP addresses are global, or common. Addresses and pools that do not have Router and DNS addresses configured within them use these global addresses.

Chapter 6: Configuring Telnet

Setting Telnet access

You can access ACLI through a Telnet session. To access ACLI remotely, the management interface 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.

```
3524GT-PWR+(config)#show telnet-access
TELNET Access:       Enabled
Login Timeout:       1 minute(s)
Login Retries:       3
Inactivity Timeout:  15 minute(s)
Event Logging:       All
Allowed Source IP Address    Allowed Source Mask
-------------------------    -------------------
1   0.0.0.0                     0.0.0.0
```

```
2   255.255.255.255             255.255.255.255
3   255.255.255.255             255.255.255.255
4   255.255.255.255             255.255.255.255
5   255.255.255.255             255.255.255.255
6   255.255.255.255             255.255.255.255
7   255.255.255.255             255.255.255.255
8   255.255.255.255             255.255.255.255
9   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] [login-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
login-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>]*	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.XXX) **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. **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 41.

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> | <dns_host_name> | <WORD> [datasize
   <64-4096>] [{count <1-9999>} |continuous] [{timeout | -t}
   <1-120>] [interval <1-60>] [debug] [source <A.B.C.D>] [ttl
   <0–255>]
   ```

   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
<*A.B.C.D* > | <*dns_host_name*> | <*WORD*>	Specifies the IP address, DNS host name, or IPv6 address of the unit to test.
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 -t parameter, 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.
source<*A.B.C.D*>	Specifies the source IP address of the packet. Must be a configured address on the switch.
ttl<*0–255*>	Specifies the maximum hop limit for the packet. Range of 0 to 255.

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

Use this procedure to display the current configuration of the switch or stack.

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*>	Displays configuration of an application for any of the following parameters: *[802.1AB] [aaur] [adac] [arp-inspection] [asset-id][aur] [banner] [core] [dhcp-relay] [dhcp-server] [dhcp-snooping] [eap] [igmp][interface] [ip] [ip-source-guard] [ipmgr] [ipv6] [l3] [l3-*

Variable	Value
	protocols] [lacp] [logging] [mac-security] [mlt] [poe] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [slamon][snmp] [ssh] [ssl] [stack] [stkmon][storm-control] [stp] [vlacp] [vlan]

IP Office Script

You can use the IPOffice script to quickly and automatically configure parameters for the ERS 3500 switch according to Avaya best practices for converged solutions. The configuration is optimized for solutions with IP Office supporting approximately 2 to 22 users on the ERS 3500 platform, and more when stacking is used.

You can execute the script with all the predefined default values and settings without the requirement of user invention. Alternatively, by using the verbose mode of the script, you have the opportunity to change the default values via prompted inputs. The script is available to all users, regardless of the access rights. The script is meant to be executed on a switch with default settings. If you execute the script on an already configured switch, you may encounter script failure or an incomplete configuration.

Table 1: Default parameters for IPOffice script

Voice VLAN ID	42
Voice VLAN 42 gateway IP	192.168.42.254
Data VLAN ID	44
Data VLAN 44 gateway IP	192.168.44.254
Switch Management IP	192.168.44.254
Default route	0.0.0.0 next hop 192.168.44.2
IP Office Call server address	192.168.42.1
IP Office File server address	192.168.42.1
Switch port 1 (or 1/1)	IP Office
Switch port 2 (or 1/2)	WAN / ADSL Router
Switch port 3 (or 1/3) & above	IP Phones, PCs, printers and other data devices

Following the port assignments, you can use the illustration below to connect your Avaya IP Office, WAN Router, IP Phones and devices to the Avaya Ethernet Routing Switch.

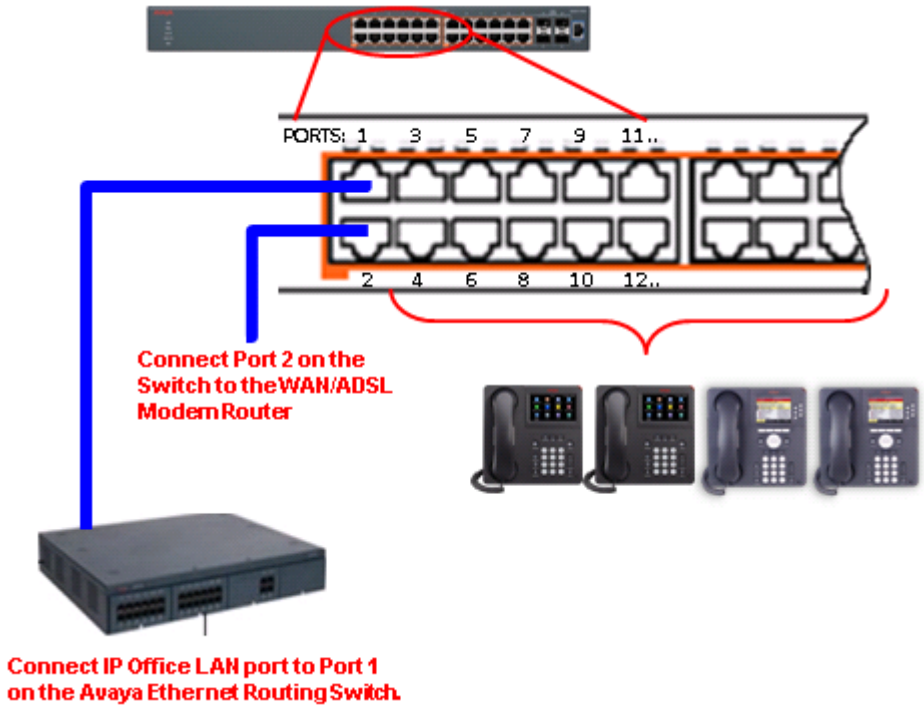


Figure 8: Connecting Avaya IP Office, Avaya IP Phones and other devices

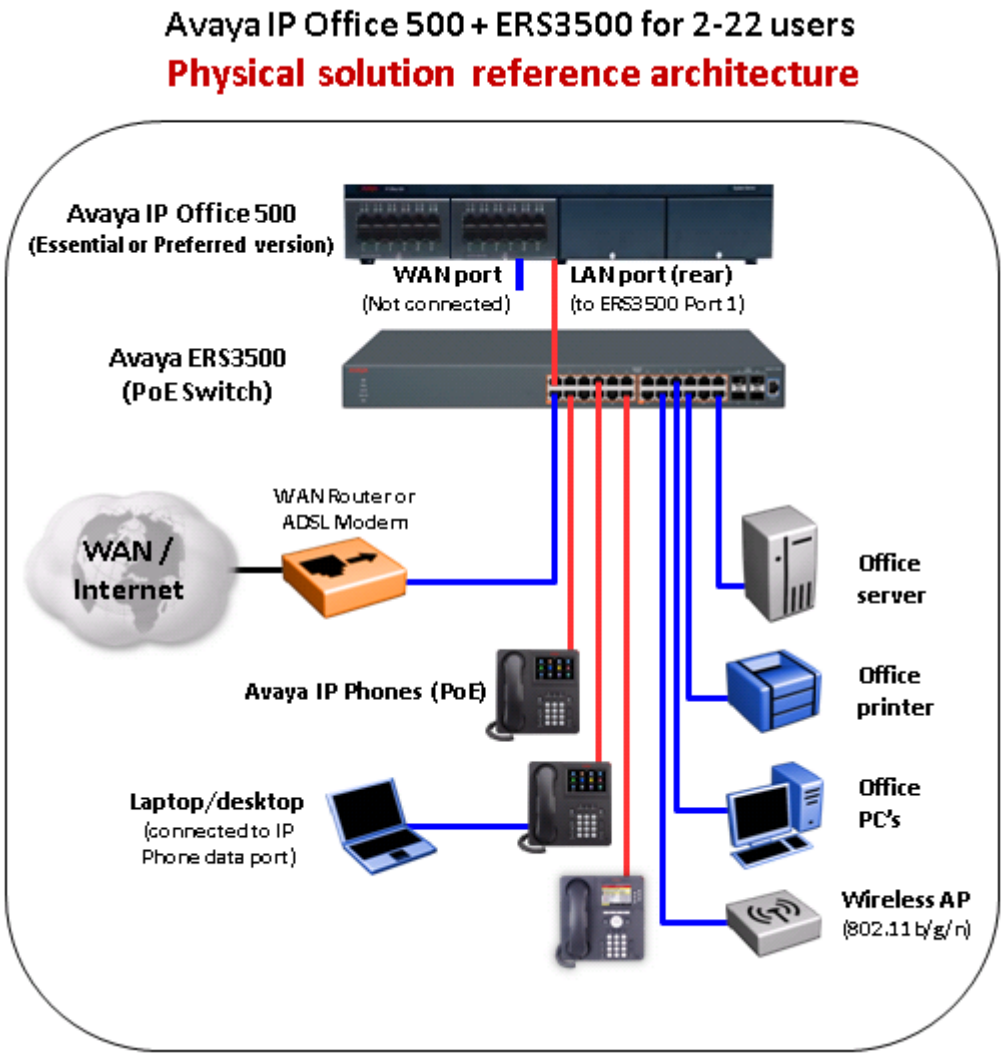


Figure 9: IP Office physical solution reference diagram

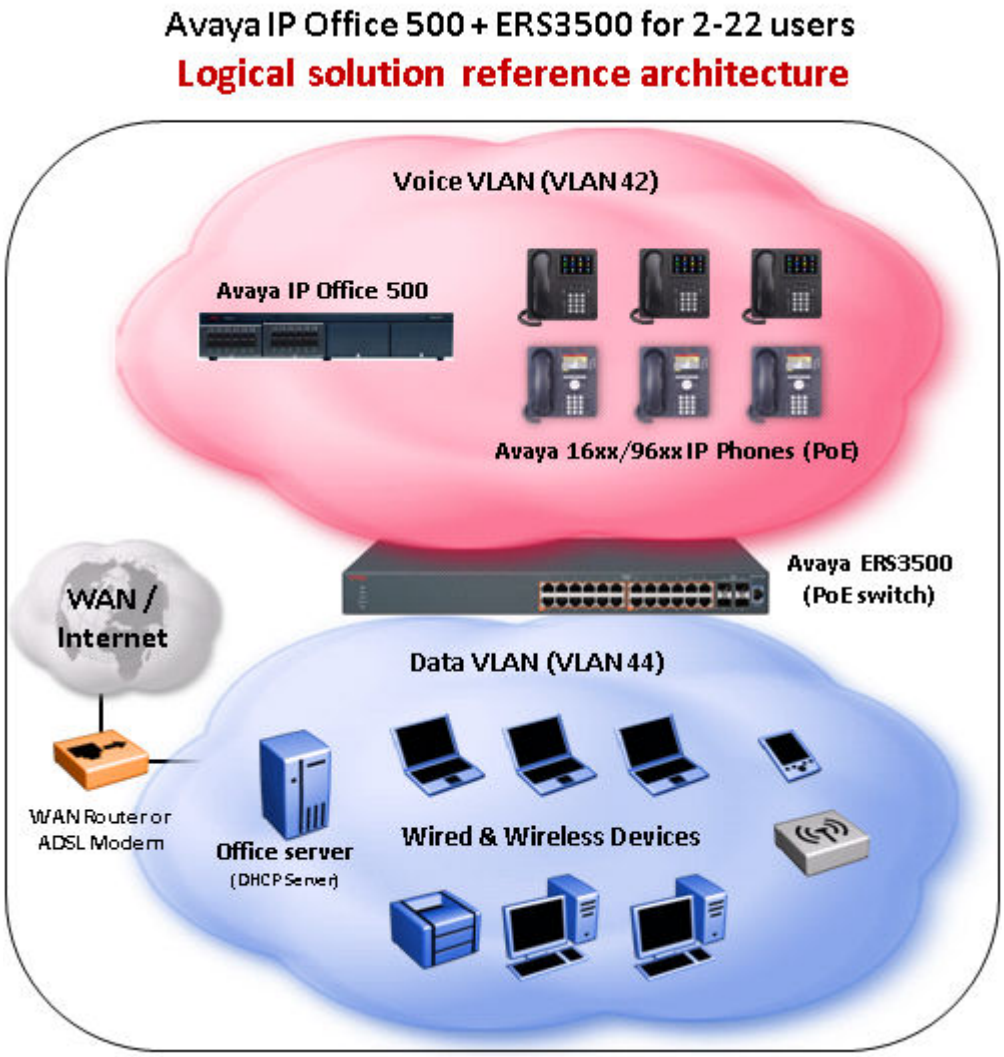


Figure 10: IP Offoce logical solution reference diagram

Configuring with IP Office Script

Use this procedure to automatically configure parameters for the ERS 3500 switch.

Before you begin

The run ipoffice command executes a script containing many switch configuration parameters to optimize the ERS 3500 switch functions for Converged IP Telephony solutions with Avaya's IP Office platform. Executing this ACLI command changes and configures a number of switch configuration options such as VLAN IDs and port memberships, VLAN IP addresses, default route, QoS and LLDP settings.

Avaya recommends that the run ipoffice ACLI commands are executed on an ERS 3500 switch operating in a factory default state.

Procedure

1. Log on to ACLI in User EXEC command mode.
2. At the command prompt, enter the following command:
   `run ipoffice [verbose]`

Example

The following is sample output of the **run ipoffice** command script

```
3526T-PWR+>en
3526T-PWR+#run ipoffice

% The Voice VLAN ID has been set to 42
% The Voice VLAN Gateway IP address has been set to 192.168.42.254
% The Voice VLAN Gateway IP network mask has been set to 255.255.255.0
% The Data VLAN ID has been set to 44
% The Data VLAN IP address has been set to 192.168.44.254
% The Data VLAN IP network mask has been set to 255.255.255.0
% ------------------------------------------------------------------------
% IP Offie LAN port is et to plug into switch port 1
% Gateway Modem-Router port is set to plug into switch port 2
% ------------------------------------------------------------------------
% Default IP Route set to 192.168.44.2 (Gateway Modem-Router interface)
% IP Office Call-Server IP address is set to 192.168.42.1
% IP Office File-Server IP address is set to 192.168.42.1
% ** Switch QoS and Unified Communications policies setup and saved **
% ** IP Office solution automated switch setup complete and saved **
% ------------------------------------------------------------------------
% To manage this Avaya switch, enter 192.168.44.254 in your Web browser.
% ------------------------------------------------------------------------
3526T-PWR+#
```

The following is sample output of the **run ipoffice verbose** command script

```
3510GT-PWR+# run ipoffice verbose

*********************************************************
*** This script will guide you through configuring the ***
*** Avaya switch for optimal operation with IP Office. ***
*** ---------------------------------------------------***
*** The values in [] are the default values, you can   ***
*** input alternative values at any of the prompts.    ***
*** Warning: This script may delete previous settings. ***
*** If you wish to terminate or exit this script       ***
*** enter ^C <control-C> at any prompt.                ***
*********************************************************
Voice VLAN ID [42] :
% The Voice VLAN ID has been set to 42
Data VLANI ID [44] :
Voice VLAN Gateway IP Address [192.168.42.254] :10.10.42.254
Voice VLAN Gateway IP Mask [255.255.255.0] :
% The Voice VLAN Gateway IP address has been set to 10.10.42.254
% The Voice VLAN Gateway IP network mask has been set to 255.255.255.0
% The Data VLAN ID has been set to 44
Data VLAN Gateway IP Address [192.168.44.254] :10.10.44.254
Data VLAN Gateway IP Mask [255.255.255.0] :
% The Data VLAN IP address has been set to 10.10.44.254
% The Data VLAN IP network mask has been set to 255.255.255.0
% IP Office LAN port is set to plug into switch port 1
% Gateway Modem-Router port is set to plug into switch port 2
```

```
IP Route to Gateway Modem-Router (Internet/WAN) [192.168.44.2] :10.10.44.99
% Default IP Route set to 10.10.44.99 (Gateway Modem-Router interface)
IP Office Call-Server IP address [192.168.42.1] :10.10.42.200
% IP Office Call-Server IP address is set to 10.10.42.200
IP Office File-Server IP address [192.168.42.1] :10.10.42.200
% IP Office File-Server IP address is set to 10.10.42.200
% ** Switch QoS and Unified Communications policies setup and saved **
% ** IP Office solution automated switch setup complete and saved **
% ------------------------------------------------------------------------
% To manage this Avaya switch, enter 10.10.44.254 in your Web browser.
% ------------------------------------------------------------------------
3510GT-PWR+#
```

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

1. 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 or Hostname>	Specifies: • the IP address of the target device in dotted-decimal notation (A.B.C.D in the format XXX.XXX.XXX.XXX) • 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:
   `[no] ip name-server <A.B.C.D>`

Variable definitions

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

Variable	Value
<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:
   `[no] [default] ip domain-name [<LINE>]`

Variable definitions

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

Variable	Value
<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).
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 enable**command.

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 | list | mode | password [type | unit <1–8>]}`

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
list	Lists CLI tree
mode	Displays information about current ACLI mode
password [type]	Displays the current password type configured for serial console and Telnet access to the stack, or standalone switch. Values include: • local — the system local password is used • none — no password is used

Variable	Value
	• radius — RADIUS password authentication is used • tacacs — TACACS+ AAA services are used
password [unit <1–8>]	Displays current ACLI user names and passwords for a specific unit or all units.

Displaying system information

Display the current system characteristics.

Important:

You must enable and configure SNTP to display GMT time. Refer to Simple Network Time Protocol (SNTP) on page 73 for more details.

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:            Switch
MAC Address:               C8-F4-06-D7-C8-00
P0E Module FW:             4.0.1B2
Reset Count:               16
Last Reset Type:           Software Download
Autotopology:              Enabled
Pluggable Port 21:         None
Pluggable Port 22:         None
Pluggable Port 23:         None
Pluggable port 24:         None
Pluggable Port 25:         None
Pluggable Port 26:         None
sysDescr:                  Ethernet Routing Switch 3524GT-PWR+
                           HW:R0B    FW:t1116  SW:v5.0.0.045
                           Mfg Date: 20111101   HW Dev:none
Serial #:                  SDNI24GTP0B001
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:               1.3.6.1.4.1.45.3.80.4
```

```
sysUpTime:                  8 days, 08:58:56
sysNtpTime:                 NTP not synchronized
sysServices:                6
sysContact:
sysName:
----More (q=Quit, space/return=Continue)----
```

Configuring LEDs to blink on the display panel

Use this procedure to set the LEDs on the display panel to blink to identify a particular unit.

Procedure

1. Log on to Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   `blink-leds [off | time <1–10> | unit <1–8>]`

Variable definitions

The following table describes the parameters for the **`blink-leds`** command.

Variable	Value
off	Sets the LEDs to stop blinking
time *<1–10>*	Indicates the duration, in minutes, for the LEDs to blink to identify the unit. RANGE: 1 to 10 minutes DEFAULT: ?
unit *<1–8>*	Specifies the unit number. RANGE: 1 to 8 units

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) with the text specified in LINE
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

Use this procedure to display the current status of all interfaces or for a specific port

The status of all port interfaces on the switch or stack can be viewed, including Mult-Link Trunk membership, link status, autonegotiation and speed.

Procedure

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

Example

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

```
3510GT-PWR+#show interfaces names 1,2,3
Port   Name
----   ----
1      LabBldg
```

```
2      Testing
3      FloorBldg
```

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

```
3524GT-PWR+#show interfaces
                Status                              Auto                          Flow
Port  Trunk   Admin   Oper   Link   LinkTrap   Negotiation Speed    Duplex  Control
----  -----   -----   ----   ----   --------   ----------- -------- ------  -------
1             Enable  Up     Up     Enabled    Custom      1000Mbps Full    Disable
2             Enable  Down   Down   Enabled    Custom
3             Enable  Down   Down   Enabled    Custom
4             Enable  Down   Down   Enabled    Custom
5             Enable  Down   Down   Enabled    Custom
6             Enable  Down   Down   Enabled    Custom
7             Enable  Down   Down   Enabled    Custom
8             Enable  Down   Down   Enabled    Custom
9             Enable  Down   Down   Enabled    Custom
10            Enable  Down   Down   Enabled    Custom
```

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

```
3524GT-PWR+#show interfaces verbose
Port:    1
     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:  Custom
     Link Speed:  1000Mbps
     Link Duplex:  Full=Duplex
     BPDU-guard (BPDU Filtering): Disabled
     BPDU-guard (BPDU Filtering): Oper Status: N/A
Port:    2
     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:  Custom
     BPDU-guard (BPDU Filtering): Disabled
     BPDU-guard (BPDU Filtering): Oper Status: N/A
----More (q=Quit, space/return=Continue)----
```

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

```
35326T#show interfaces link-up
                Status                              Auto                          Flow
Port  Trunk   Admin   Oper   Link   LinkTrap   Negotiation Speed    Duplex  Control
----  -----   -----   ----   ----   --------   ----------- -------- ------  -------
1             Enable  Up     Up     Enabled    Enabled     100Mbps  Full    Disable
3             Enable  Up     Up     Enabled    Enabled     100Mbps  Full    Disable
```

```
13            Enable  Up     Up     Enabled    Enabled     100Mbps  Full    Disable
```

Variable definitions

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

Variable	Value
admin-disabled	Displays the interfaces with administration disabled.
admin-enabled	Displays the interfaces with administration enabled.
gbic-info	Displays Gigabit Interface Converter (GBIC) details.
link-down	Displays the interfaces with link down.
link-up	Displays the interfaces with link up.
names	Displays the interface names.
verbose	Displays full information about each port.
<*portlist*>	Specifies the ports that you want to display.

Displaying interface configurations

Use this procedure to display the current configuration of all interfaces or for a specific port.

The configuration of all port interfaces on the switch or stack can be viewed, including port configuration, VLAN interface, VLAN port member, and Spanning-Tree configuration.

Procedure

1. Log on to ACLI in User 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.

```
35326-PWR+>#show interfaces 1/1 config
Unit/Port:    1/1
     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
     Link Speed:  100Mbps
     Link Duplex:  Full-Duplex
     Flow Control:  Disable
     BPDU-guard (BPDU Filtering): Disabled
     BPDU-guard (BPDU Filtering): Oper Status: N/A

*****VLAN interfaces configuration*****
           Filter     Filter
          Untagged Unregistered
Unit/Port  Frames     Frames    PVID PRI    Tagging    Name
--------- -------- ------------ ---- --- ------------ ----------------
1/1       No       Yes          1    0   UntagAll     Unit 1,Port 1

(((((VLAN ID port member configuration*****
Unit/Port VLAN VLAN Name        VLAN VLAN Name        VLAN VLAN Name
--------- ---- ---------------- ---- ---------------- ---- ----------------
1/1       1    VLAN #1
--------- ---- ---------------- ---- ---------------- ---- ----------------

*****Spanning-tree port configurations*****
Unit Port Trunk   Participation   Priority  Path Cost    State
---- ---- -----  ---------------  --------  ---------  ----------
1    1           Normal Learning  128       10         Forwarding
35326-PWR+>
```

Variable definitions

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

Variable	Value
<portlist.>	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
SNTP Status:                    Disabled
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:    0
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 <primary|secondary> address`** command.

Variable	Value
<A.B.C.D>	Enter the IP address of the primary or secondary NTP server in the format XXX.XXX.XXX.XXX. DEFAULT: 0.0.0.0.
no	Clears the NTP server IP addresses
<primary|secondary>	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

Variable	Value
date *{<day> <month> <year> <hh:mm>} {<day> <month> <year> <hh:mm>}*	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>.
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>	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>	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>	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)#
```

Enabling or disabling UTC timestamp in ACLI show command outputs

Use this procedure to enable or disable the display of the UTC timestamp in ACLI show command outputs. The default, the timestamp state is disabled.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. To enable the display of the UTC timestamp, enter the following command:
   `cli timestamp enable`
3. To disable the display of the UTC timestamp, enter the following command:
   `no cli timestamp enable`

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

Setting stack forced mode

This section describes the procedures and commands to configure and display stack forced mode on a two unit stack.

Enabling or disabling stack forced mode

Use this procedure to enable or disable stacked forced mode on a two unit stack.

Before you begin

Stack Forced Mode requires a stack configuration of two units.

About this task

You can use Stack Forced Mode to manage one of the stand-alone units from a broken stack of two with the previous stack IP address. When Stack Forced Mode is enabled, it only activates if the stack fails.

Procedure

1. Log on to Global Configuration mode in ACLI.
2. To enable Stack Forced Mode, enter the following command:

```
stack forced-mode
```

3. To disable Stack Forced Mode, enter the following command:
   ```
   no stack forced-mode
   ```
4. To default Stack Forced Mode, enter the following command:
   ```
   default stack forced-mode
   ```
   The default is disabled.

Variable definitions

The following table describes the parameters for the **`stack forced-mode`** command.

Variable	Value
no	Disables stack forced-mode

Displaying stack forced-mode

Use this procedure to display the stack forced mode status for the switch. If the status is Enabled, the device is currently running in stack forced mode. If the status is Disabled, the device is not running in stack forced mode.

Before you begin

Stack Forced Mode requires a stack configuration of two units.

Procedure

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

Example

The following figure provides a sample of the **`show stack forced-mode`** command.

```
3526T-PWR+<config>#show stack forced-mode
Forced-Stack Mode: Disabled
Device is not currently running in forced stack mode.
3526T-PWR+<config>#
```

Configuring the operational mode on rear ports

Use this procedure to configure the operational mode of rear ports into Stacking or Standalone Mode.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   `rear-ports mode {standalone | stacking}`

Variable definitions

The following table describes the parameters for the **`rear-ports mode`** command.

Variable	Value
{standalone | stacking}	Specifies the operational mode of the rear facing ports of the selected unit as Standalone or Stacking. DEFAULT: Standalone

Displaying operational mode of the rear port

Use this procedure to display the operational mode of the rear port on a switch in Standalone or Stacking Mode.

Procedure

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

Example

The following figure provides a sample of the **`show rear-ports mode`** command.

```
3526T-PWR+<config>#show rear-ports mode
Current rear-ports mode: Stacking Mode
```

```
Next rear-ports mode: Stacking Mode
Next mode will be applied after reset
3526T-PWR+<config>#
```

AUR configuration

This section describes ACLI commands used in Auto Unit Replacement (AUR) configuration.

Enabling or disabling AUR

Use this procedure to enable or disable AUR on the switch, or to set the AUR configuration to the default value.

Procedure

1. Log on to Global Configuration mode in ACLI.
2. To enable AUR, enter the following command:
   `stack auto-unit-replacement enable`
3. To disable AUR, enter the following command:
   `no stack auto-unit-replacement enable`
4. To default AUR, enter the following command:
   `default stack auto-unit-replacement enable`

Displaying AUR

Use this procedure to displays the current AUR settings.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   `show stack auto-unit-replacement`

Example

The following figure provides a sample of the **`show stack auto-unit-replacement`** command.

```
3526T-PWR+<config?#show stack auto-unit-replacement
Auto Unit Replacement Auto-Resorte: Enabled
```

```
Auto Unit Replacement Auto-Save:   Enabled

UNIT #         LAST CONFIG-SAVE TIME-STAMP         READY FOR REPLACEMENT
1                     3 days 10:23:02                      Yes
2                     0 days 00:01:40                      NO
3                     3 days 10:12:33                      Yes
6                     3 days 10:12:34                      NO
8                     3 days 10:12:35                      Yes
```

Enabling or disabling AUR configuration saves

Use the following commands to enable or disable AUR automatic configuration saves.

Before you begin

AUR requires a stack configuration

About this task

You can configure AUR to enable or disable automatic configuration saves for non-base units.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. To enable AUR automatic configuration saves, enter the following command:
   `stack auto-unit-replacement config save enable`
3. To disable AUR automatic configuration saves, enter the following command:
   `stack auto-unit-replacement config save disable`

Removing MAC addresses from AUR cache

Use the following procedure to remove a MAC address from the AUR cache for a non-operational unit.

Before you begin

AUR requires a stack configuration.

You require a stack of at least three units.

About this task

You can remove the MAC address of a non-operational stack unit from the Auto Unit Replacement (AUR) cache. A non-operational unit can be a switch that is no longer present in the stack, or a stack switch that is being restored within the stack. When you remove the MAC address information of the non-operational unit from the AUR cache, the hardware information is retained in the AUR cache. The next unit joining a stack that matches the unit

hardware can replace the non-operational unit, regardless of the MAC address. You cannot remove the MAC address of operational units.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. To verify that the stack unit is non-operational, enter the following command:
   `show stack auto-unit-replacement mac-addresses`
3. To remove the MAC address of a non-operational unit, enter the following command:
   `stack auto-unit-replacement remove-mac-address unit <1-8>`

Example

Verify the operational status of the stack.

```
show stack auto-unit-replacement mac-addresses

UNIT #          PHYSICAL ADDRESS                OPERATIONAL

Unit 1          00-1C-9C-4A-78-00                       YES

Unit 2          00-1A-8F-E7-38-00                       YES

Unit 3          00-1C-9C-BB-74-00                       YES
```

You cannot remove the MAC address of an operational unit. Prepare the unit for replacement, remove the unit from the stack, and verify the operational status.

```
show stack auto-unit-replacement mac-addresses

UNIT #          PHYSICAL ADDRESS                OPERATIONAL

Unit 1          00-1C-9C-4A-78-00                       YES

Unit 2          00-1A-8F-E7-38-00                       YES

Unit 3          00-1C-9C-BB-74-00                       NO
```

Remove the MAC address for the non-operational unit.

```
stack auto-unit-replacement remove-mac-address unit 3
```

Verify that the MAC address is deleted for the non-operational unit.

```
show stack auto-unit-replacement mac-addresses

UNIT #          PHYSICAL ADDRESS                OPERATIONAL

Unit 1          00-1C-9C-4A-78-00                       YES

Unit 2          00-1A-8F-E7-38-00                       YES

Unit 3          00-00-00-00-00-00                       NO
```

Add a new unit with a matching hardware configuration to the stack. Regardless of the new unit MAC address, the AUR configuration copies to the new unit and the new unit reboots. Once booted, the new unit joins the stack.

Displaying stack information

Use this procedure to display the current stack information. In addition, it will cause the front face LEDs to light up to display the unit ID. For example, unit 4 will light LEDs 1 through 4.

Procedure

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

Example

The following figure provides a sample of the **`show stack-info`** command.

```
TO BE ADDED
```

AAUR configuration

Use ACLI procedures in the following sections to manage and configure Agent Auto Unit Replacement (AAUR). You can currently manage this functionality only through ACLI.

Enabling or disabling AAUR

Use this procedure to enable or disable Agent Auto Unit Replacement (AAUR).

Note:

AAUR is recommended and enabled by default.

Before you begin

AAUR requires a stack configuration

About this task

You can use the Agent Auto Unit Replacement (AAUR) feature to ensure that all units in a stack run the same software image.

Procedure

1. Log on to the Global configuration mode in ACLI.
2. To enable AUR, enter the following command:
   ```
   stack auto-unit-replacement-image enable
   ```

   Note:

   Diagnostic Auto Unit Replacement (DAUR) is configured with AAUR. There are no commands to separately enable or disable DAUR.
3. To disable AUR, enter the following command:
   ```
   no stack auto-unit-replacement-image enable
   ```
4. To default AUR, enter the following command:
   ```
   default stack auto-unit-replacement-image enable
   ```

   The default is enabled.

Displaying AAUR configuration

Use this procedure to view the AAUR configuration.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show stack auto-unit-replacement-image enable
   ```

   Note:

   Diagnostic Auto Unit Replacement (DAUR) is configured with AAUR. There are no commands to separately display DAUR.

Example

The following figure provides a sample of the **`show stack auto-unit-replacement-image`** command.

```
3526T-PWR+<config?#show stack auto-unit-replacement-image
Auto Unit Image Replacement:  Enabled
```

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:
   `[no] [default] tftp-server [<A.B.C.D> | <WORD>]`

Variable definitions

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

Variable	Value
<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.
<*WORD*>	Specifies the IPv6 address of the server you want to use for TFTP services.
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 not 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 Privileged EXEC mode in ACLI.
2. To display the current autonegotiation advertisements, enter the following command:

   ```
   show auto-negotiation-advertisements [port <portlist>]
   ```

Example

```
3526T-PWR+#show auto-negotiation-advertisements port 1/20-26
Unit/Port   Autonegotiation Advertised Capabilities
---------   ---------------------------------------------------------------------
1/20        10Full 10Half 100Full 100Half
1/21        10Full 10Half 100Full 100Half
1/22        10Full 10Half 100Full 100Half
1/23        10Full 10Half 100Full 100Half
1/24        10Full 10Half 100Full 100Half
1/25        10Full 10Half 100Full 100Half 1000Full              AsymmPause
1/26        10Full 10Half 100Full 100Half 1000Full              AsymmPause
3526T-PWR+#
```

Variable definitions

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

Variable	Value
port<*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>]
   ```

Example

```
3526T-PWR+#show auto-negotiation-capabilities port 1/20-26
Unit/Port   Autonegotiation  Capabilities
---------   ------------------------------------------------------------------
1/20        10Full 10Half 100Full 100Half
1/21        10Full 10Half 100Full 100Half
1/22        10Full 10Half 100Full 100Half
1/23        10Full 10Half 100Full 100Half
1/24        10Full 10Half 100Full 100Half
1/25        10Full 10Half 100Full 100Half 1000Full              AsymmPause
1/26        10Full 10Half 100Full 100Half 1000Full              AsymmPause
3526T-PWR+#
```

Variable definitions

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

Variable	Value
port<*portlist*>	Enter ports for which you want the current autonegotiation capabilities 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 or stack, 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*>	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. **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*>	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>	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.
2. At the command prompt, enter the following command:
   `[default] speed [port <portlist>] {10|100|1000|auto}`

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*>	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*>	Specifies the port number to configure the duplex mode. Enter the port number you want to configure, or ALL to configure all ports simultaneously. **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 set the flow control mode to Asymmetric or disabled.

Asymmetric mode

This mode lets the link partner send flow control pause frames to the Gigabit Ethernet 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 port is disabled from transmitting pause frames to its link partner. Use this mode when the 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.

About this task

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

Note:

You can activate flow control as follows:

- if auto-negotiation is enabled on the port, you must activate asymm-pause-frame advertisement for that port to autonegotiate both the speed/duplex of the link as well as the flow control setting
- if auto-negotiation is disabled on the port, you need to use the *asymmetric* parameter of the flowcontrol command

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 |
auto | disable}
```

Variable definitions

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

Variable	Value
port <*portlist*>	Specifies the port numbers to use for flow control

Variable	Value
	Important: If you omit this parameter, the system uses the port number you specified in the **`interface`** command.
asymmetric | auto | disable	Sets the mode for flow control: • asymmetric — enables the local port to perform flow control on the remote port • auto — enables auto-negotiation on the specified port and flow control status will be determined after the auto-negotiation process completes, depending on the currently activated auto-negotiation advertisements • 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.

Note:

With the Storm Control feature added in Release 5.1, both Storm Control and Rate Limiting are disabled by default. Only one of these features can be enabled at any one time. In order to use Rate Limiting, you must ensure that Storm Control is globally disabled.

Displaying rate-limit configuration using ACLI

Display rate-limit configuration to view settings and statistics.

Procedure

1. 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 or stack
default	Restores the default value for rate limiting for the switch or stack

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: 802dot3at_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.

Procedure

1. Log on to ACLI in Privileged Exec command mode.
2. At the command prompt, enter the following command:
   `show poe-main-status [unit <1–8>]`

Example

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

```
3524GT-PWR+>enable
3524GT-PWR+#show poe-main-status
PoE Main Status - Stand-alone
----------------------------
Available DTE Power        : 370 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
```

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

Procedure

1. Log on to ACLI in Privileged Exec command mode.
2. At the command prompt, enter the following command:
   `show poe-port-status [<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
2     Enable  Invalid PD  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     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
----More (q=Quit, space/return=Continue)----
```

Variable definitions

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

Variable	Value
<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.

Procedure

1. Log on to ACLI in Privileged Exec command mode.
2. At the command prompt, enter the following command:
   `show poe-power-measurement [<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)  Current(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
<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

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

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

The default is: High Power Budget Mode (Normal mode, fan operates).

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 Setting a power usage threshold on page 106. 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 budget 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}`

Note:

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

Example

The following figure provides a sample output of the **`show poe-main-status`** command showing PoE power mode settings.

```
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 budget 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

Use the following procedure to display the PoE budget operating mode for the ERS 3510GT-PWR+ switch. There are 2 power budget modes; low (Fanless) or high (Normal).

The default is: high power budget mode (Normal mode, fan operates).

Procedure

1. Log on to ACLI in Privileged Exec command mode.
2. At the command prompt, enter the following command:
   `show poe-main-status`

Example

The following figure provides a sample of the **show poe-main-status** 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
```

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.

Caution:

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:

Unless the no-reset option is selected, 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, unless the no-reset option is selected. 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*>	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*>	Enter the name of the Ethernet Routing Switch 3500 Series software image you want to download.
image-if-newer <*image-name*>	Enter the name of the Ethernet Routing Switch 3500 Series software image of the newer version you want to download.
diag <*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.

Show software status

You can display the currently loaded and operational switch or stack 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 diagnostic software load

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

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 diagnostic load only.
image	Displays information for the image load only.

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 be 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.

⚠ Caution:

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 nvram** to save the new configuration.
- Enter **reload cancel** to cancel the previous reload command.

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 *minutes-to-wait <1–60>* parameter.

Chapter 13: Configuring the switch using EDM

Configuring Quick Start using EDM

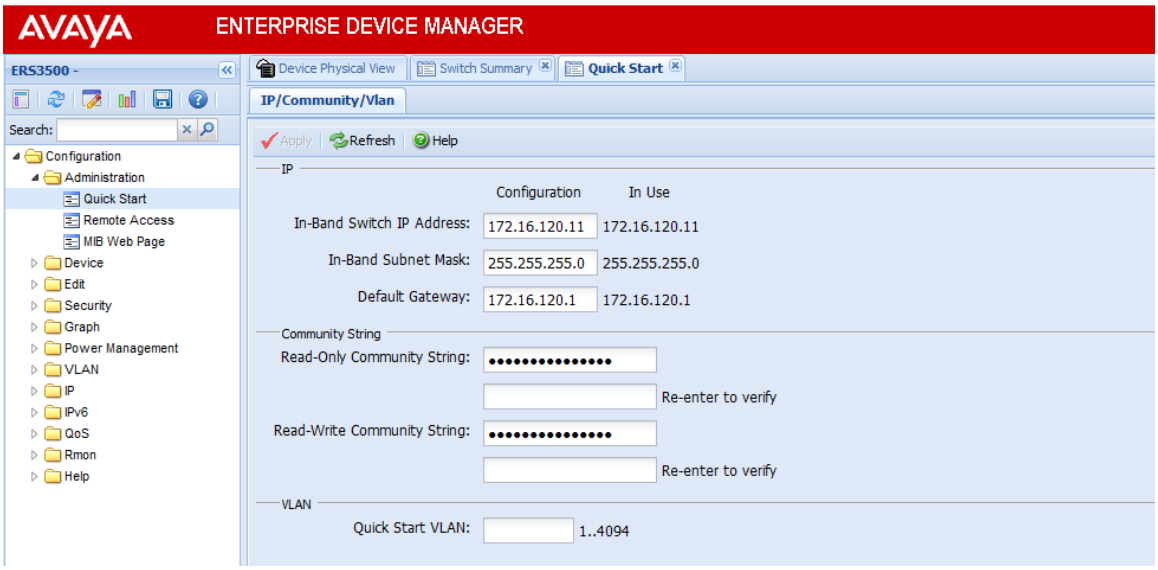
Perform this procedure to configure Quick Start to enter the setup mode through a single screen.

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.

Procedure

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
Type	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 interface ports

Use the following procedure to configure one or more interface ports.

Before you begin

You must select one or multiple ports from the **Device Physical View** tab.

About this task

You can view and configure the configuration for the interface ports on the switch or stack.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Ports**.
4. In the work area, click the **Interface** tab.
5. To select an interface port to edit, click a port row the **Index** column.

6. In the port row, double-click the cell in the **Name** column, type a character name.
7. In the port row, double-click the cell in the **AdminStatus** column and select a value from the list.
8. In the port row, double-click the cell in the **LinkTrap** column and select a value from the list.
9. In the port row, double-click the cell in the **AutoNegotiate** column and select a value from the list.
10. In the port row, double-click the cell in the **AdminDuplex** column and select a value from the list.
11. In the port row, double-click the cell in the **AdminSpeed** column and select a value from the list.
12. Repeat steps 5 through 11 to configure additional interface ports.
13. On the toolbar, click **Apply**.
14. To view and verify the current configuration, click **Refresh**.

Variable definitions

The following table describes configuring interface ports.

Variable	Value
Index	Indicates a unique value assigned to each interface port.
Name	Specifies a name for the port.
Descr	Indicates the description for the port.
Type	Indicates the media type for the port.
Mtu	Indicates the size of the largest packet that can be sent or received, in octets.
PhysAddress	Indicates the MAC address assigned to the port.
AdminStatus	Specifies the current administrative state of the port. Values include: • up • down All ports start in an up state on a managed system. The AdminStatus changes do down

Variable	Value
	due to administrator action or the configuration information.
OperStatus	Indicates the current operational state of the port. Values include: • up — port is ready to transmit and receive traffic • down — port is not ready to transmit and receive traffic • testing — port is currently being tested
LastChange	Indicates the value of sysUpTime at the time the interface entered into the current state. If the current state occurred before the last reinitialization of the local management subsystem, the value is zero.
LinkTrap	Specifies if traps are generated for this port.
AutoNegotiate	Specifies if Autonegotiation is enabled or disabled on the port.
AdminDuplex	Specifies the duplex mode of the port. Values include: • half • full
OperDuplex	Indicates the current duplex mode of the port.
AdminSpeed	Specifies the speed of the port. Values include: • mbps10 • mbps100 • mbps1000 • mbps10000
OperSpeed	Indicates the current speed of the port.
FlowControlAdminMode	Specifies the flow control mode of the port. Values include: • disabled — flow control disabled • enabledXmit — transmit enabled

Variable	Value
	• enabledRcv — receive enabled • enabledXmitAndRcv — transmit and receive enabled
FlowControlOperMode	Indicated the current flow control mode of the port.
AutoNegotiationCapability	Indicates the current auto negotiation capability of the port.
AutoNegotiationAdvertisements	Specifies the custom auto negotiation advertisements of the port Values include: • 10Half • 10Full • 100Half • 100Full • 1000Half • 1000Full • 10000Full • PauseFrame • AsymmPauseFrame
MltId	Indicates the MultiLink Trunk assigned to the port.
IsPortShared	Indicates whether the port is shared.
PortActiveComponent	Indicates the port components active for a shared port.

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 area, 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.

Name	Description
Reboot	Options include: • **running**: the switch remains in the running mode (default) • **reboot** : initiates a hardware reset.
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 • **dhcpAlways**: 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.

Name	Description
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.
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 or stack.

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**.
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
Type	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.

Configuring AUR

Use this procedure to enable or disable AUR on the switch.

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 **AUR** tab.

5. To enable Auto Unit Replacement, select the **AutoUnitReplacementEnabled** check box.
6. To enable Auto Unit Replacement saving, select the **AutoUnitReplacementSaveEnabled** check box.
7. Enter a value for forced saves in the **AutoUnitReplacementForceSaves** field.
8. Enter a value for AUR restore in the **AutoUnitReplacementRestore** field.
9. Click **Apply**.

AUR tab field descriptions

The following table describes the fields on the AUR tab.

Name	Description
AutoUnitReplacementEnabled	Specifies whether AUR is enabled.
AutUnitReplacementSaveEnabled	Specifies whether AUR Save is enabled.
AutUnitReplacementForceSave	Specifies whether an immediate save of the new base unit (NBU) configuration to the base unit (BU) is forced.
AutUnitReplacementRestore	Specifies whether the configuration of a unit from the saved configuration on the base unit is restored.

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**.
2. 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**.

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.

Name	Description
	• **dnldImg**: downloads a new software image to the switch. • **dnldImgIfNewer**: downloads a new software image to the switch only if it is newer than the image currently saved on FLASH. • **dnldImgNoReset**: downloads a new software image to the switch, but does not 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 diagnostic software load status using EDM

Use this procedure to display the currently saved and operational software status for agent and diagnostic 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.

Boot Image tab field descriptions

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

Name	Description
Unit # Software Image version	Indicates the operational agent software image for the switch.
Unit # Software Image in flash	Indicates the saved agent software image for the switch.
Unit # Diag Image version	Indicates the operational diagnostic software image for the switch.
Unit # Diag Image in flash	Indicates the saved 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 read-only 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 TIme 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.

Rear ports mode configuration

Use the procedures in this section to display and configure the rear ports operational mode for a standalone switch or a stack.

Configuring the rear ports mode

Use this procedure to display and configure the rear ports operational mode for a standalone switch or a stack.

Procedure

1. From the Device Physical View, select a unit.
2. In the navigation tree, double-click **Edit**.
3. From the Edit tree, click **Unit**.
4. In the work area, select the **Rear Ports Mode** tab.
5. In the **RearPortAdminMode** section, click a radio button.

Important:

A switch restart is required in order for the operational mode to take effect.

Rear Ports Mode field descriptions

The following table describes the fields on the Rear Ports Mode tab.

Name	Description
RearPortAdminMode	Specifies the rear ports operational mode. Values include: • **standalone**: selects the standalone operational mode for the rear ports • **stacking**: selects the stacking operational mode for the rear port DEFAULT: standalone
RearPortOperMode	Displays the configured operational mode of the rear ports.

Configuring a switch stack base unit

Use this procedure to configure a stack base unit and to display base unit information.

Before you begin

When physically cabling up a switch stack, only one switch must have the Base Unit Select switch set to the Base position and this switch becomes the Base Unit for the stack.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Base Unit Info** tab.
5. In the **AdminStat** section, click a radio button.
6. In the **Location** section, type a character string.
7. On the toolbar, click **Apply**.

Base Unit Info field descriptions

The following table describes the fields on the Base Unit Info tab.

Name	Description
Type	Indicates the switch type
Descr	Describes the switch hardware, including number of ports and transmission speed
Ver	Indicates the switch hardware version number
SerNum	Indicates the switch serial number
LstChng	Indicates the value of sysUpTime at the time the interface entered its current operational state. If you entered the current state prior to the last reinitialization of the local network management subsystem, the value is zero.
AdminState	Specifies the administrative state of the base unit switch. Values are **enable** or **reset**.
OperState	Indicates the operational state of the switch

Name	Description
Location	Specifies the physical location of the switch
RelPos	Indicates the relative position of the switch
BaseNumPorts	Indicates the number of base ports of the switch
TotalNumPorts	Indicates the total number of ports on the switch
IpAddress	Indicates the base unit IP address
RunningSoftwareVer	Indicates the version of the running software

Displaying pluggable ports

Use this procedure to display pluggable ports installed on your switch or stack.

Procedure

1. In the navigation tree, double-click **Edit**.
2. From the Edit tree, click **Chassis**.
3. From the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Stack Info** tab.
5. In the work area, click a unit in the **Indx** column.
6. To display the Pluggable Ports tab, on the toolbar, click **Pluggable Ports**.

Stack Info field descriptions

The following table describes the fields on the Stack Info tab.

Name	Description
Unit	Displays the stack unit number where the pluggable ports are installed
Port	Displays the port number in the unit where the pluggable port is installed
PortType	Displays the port type
VendorName	Displays the pluggable port vendor name
VendorOUI	Displays the pluggable port vendor's OUI

Name	Description
VendorPartNo	Displays the vendor's part number for the pluggable port
VendorRevision	Displays the vendor's revision number for the pluggable port
VendorSerial	Displays the vendor's pluggable port serial number
HWOptions	Displays hardware options, if present, for the pluggable port
DateCode	Displays the date code for the pluggable port
VendorData	Displays vendor data for the pluggable port
OrderCode	Displays the order code for the pluggable port

Renumbering stack switch units

Use this procedure to change the unit numbers of switches in a stack.

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Stack Numbering** tab.
5. In the unit row, double-click the cell in the **New Unit Number** column.
6. Select a value from the list.
7. On the toolbar, click **Apply**.
   A warning message appears indicating that initiating the renumbering of switch units in a stack results in an automatic reset of the entire stack.

Stack Numbering field descriptions

The following table describes the fields on the Stack Numbering tab.

Name	Description
Current Unit Number	Identifies the current switch numbering sequence

Name	Description
New Unit Number	Identifies the updated switch numbering sequence

Displaying stored content

Use this procedure to display information about files stored on the switch or stack.

Procedure

1. In the navigation tree, click **Edit**.
2. From the Edit tree, click **Chassis**.
3. From the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Store Content** tab.

Store Content field descriptions

The following table describes the fields on the Store Content tab.

Name	Description
Indx	Displays the file index number
Type	Displays the file storage type
CurSize	Displays the current size of the file storage
CntntVer	Displays the file version in storage
Filename	Displays file names for the stored content

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. In the **PoweredDeviceDetectType** section, click a radio button.
7. 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.

Name	Description
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.
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** - detection method outlined in IEEE 802.3af draft standard • **802.3af and legacy support** - detection standard in use prior to IEEE 802.3af draft standard • **802.3at** - IEEE standard for higher PoE (PoE+) • **802.3at and legacy support** -standard in use prior to IEEE 802.at **Important:** The default setting is 802.3at and legacy support. Ensure that this setting matches the setting for the detection type used by the powered devices on this switch.
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 **Power Management**.
2. In the Power Management tree, click **PoE**.
3. In the work area, click the **PoE Ports** tab.

PoE tab field descriptions

The following table describes the fields on the PoE Ports 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 • **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.

Name	Description
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: 32 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 Budget Mode
- Normal mode — High Power Budget Mode

The default is: High Power Budget Mode (Normal mode, fan operates).

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 Managing switch PoE using EDM on page 151. In Normal mode, the PoE budget is not limited; a maximum of 170 Watts is available.

Use this procedure to set the PoE power budget 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 Budget Mode and disable fan operation, select the **lowPowerBudget** checkbox.

   OR

   - To enable High Power Budget 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 budget 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, fan operates)

Appendix A: Configuring VLANs for voice and data

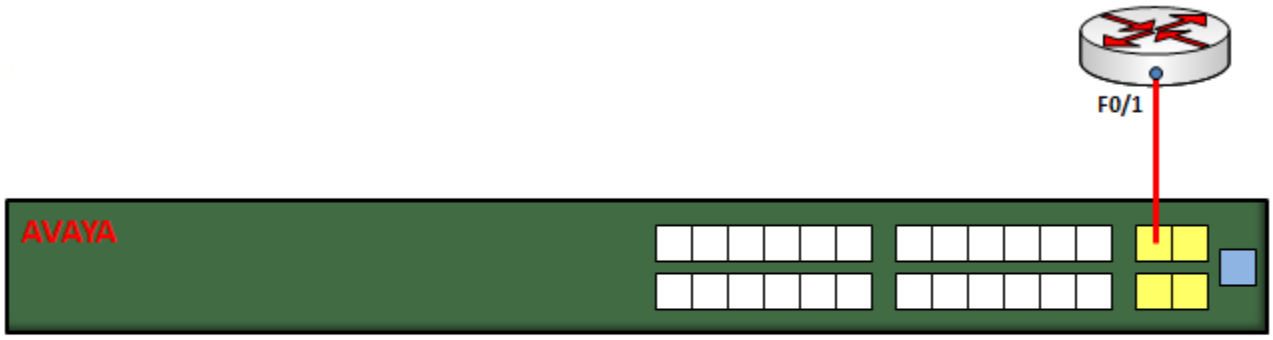
Before you begin

Connect the PC or laptop to the switch using the DB-9 male to RJ-45 serial cable.
Power the switch on.
Access CLI using ProComm or other terminal emulation software.
Ensure that the switch is set to factory default settings

About this task

In this scenario, a customer wants to install the **Avaya 3526T-PWR** and eventually connect the switch to their network via 802.1q tagging. This section provides an example of setting up the switch to access the WebGui and how to use the Enterprise Device Manager to configure VLANs for voice and data traffic on the Ethernet Routing Switch 3500 Series switch or stack.

On completion of the procedures in this example, the switch will be configured as shown in the following illustration.

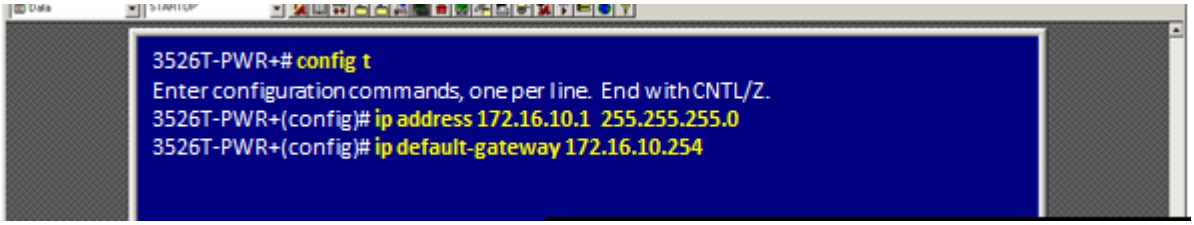


Procedure

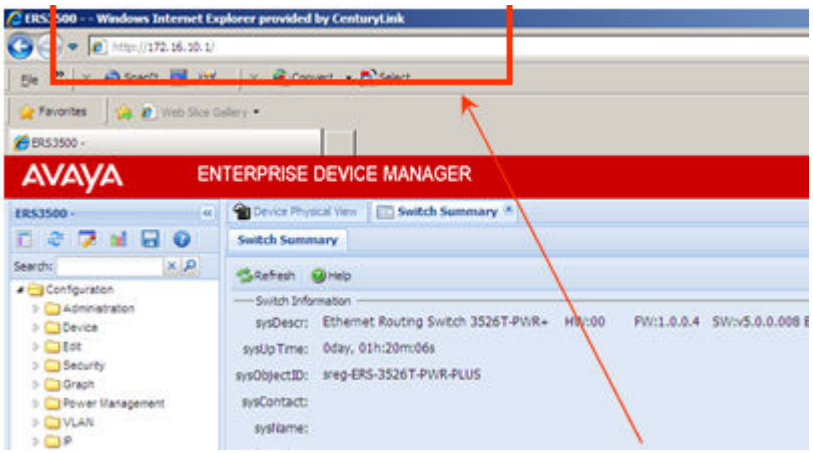
1. At the Avaya ERS CLI page, press **ctrl + y** to start the session.
2. Enter the command **Enable**.

# indicates you have successfully switched to the privileged administrator mode of operation.

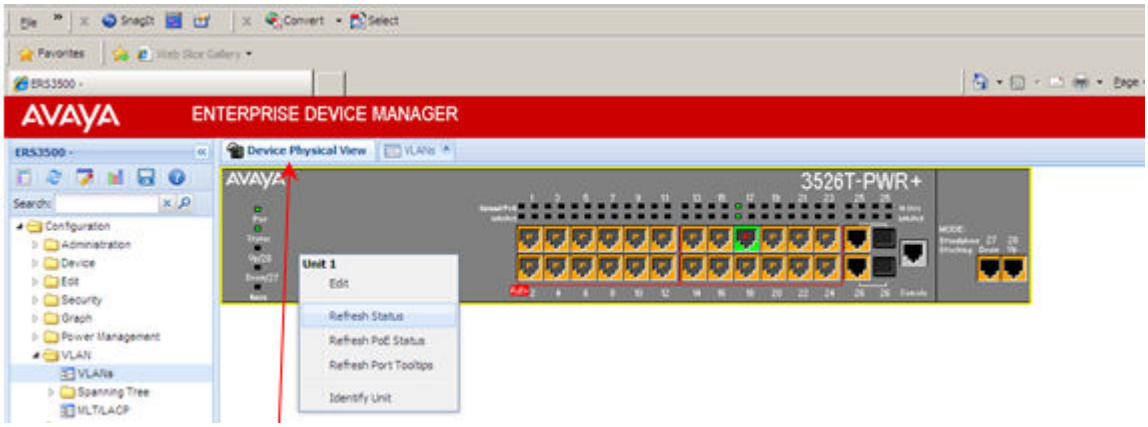
3. At the ERS CLI, enter the command **config t**.
   User is prompted to enter configuration commands.
4. Input the desired VLAN management IP address and subnet. In this example the IP address for the switch will be set to the 172.16.10.0 / 24 sub-network.
5. Press Enter.
6. Input the desired VLAN management IP default gateway.
7. Press Enter.



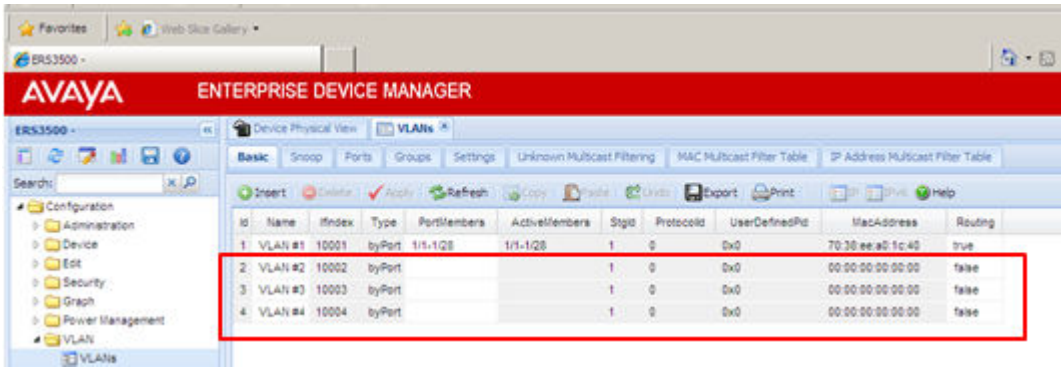
8. Using IE, navigate to the address of the management VLAN : 172.16.10.1 .
   The ERS-3500 web GUI appears.



9. In theThe ERS-3500 web GUI navigate to **Device Physical View**.

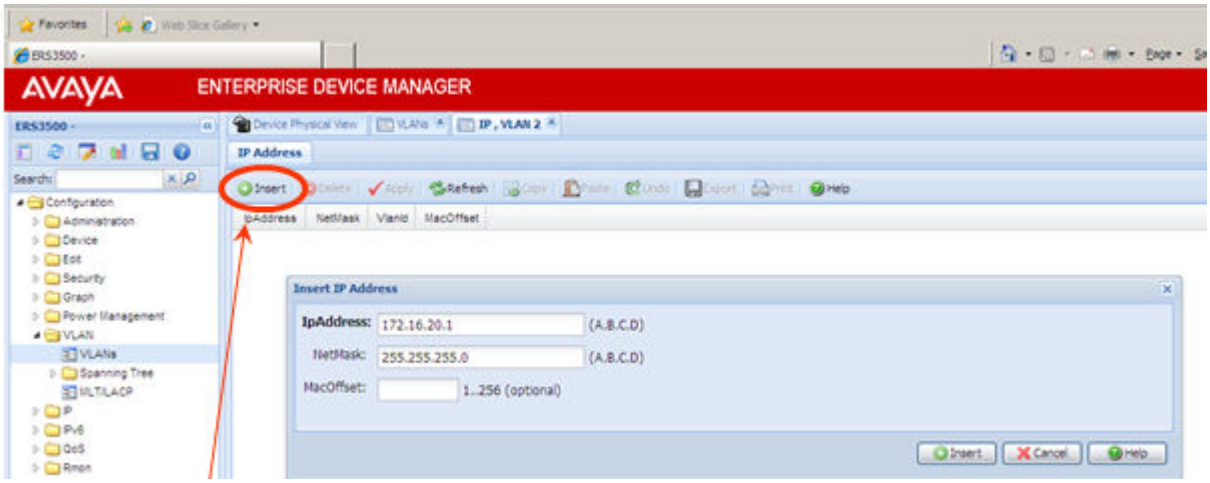


10. Select the VLANs tab.
11. Click **Insert** to start adding the new VLANs.
12. Choose the desired VLAN ID.
13. Provide a VLAN name and select the VLAN type of **byPort**.
14. Click insert when done to add the VLAN.
15. Click apply to complete the addition of the VLAN.
16. Repeat steps 3 through 7 to add additional VLANs.



Note that the new VLANs do not have any assigned ports and routing is set to false.

17. From the VLANs tab of the WebGui, click to select the desired VLAN.
    In this example, VLAN 2 will be selected.
18. Click **IP**.
    the new tab of **IP, VLAN-2** opens.

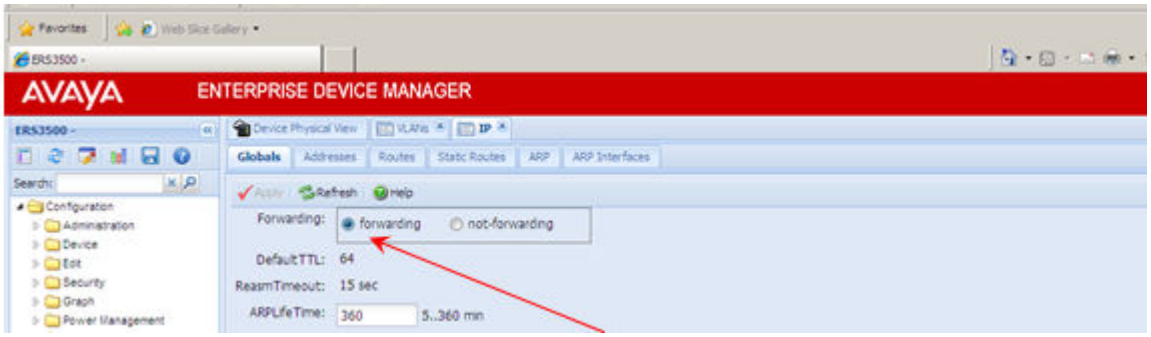


19. Click **Insert**.
20. Input the desired **IP address** and **subnet mask**.
21. Click **insert** to complete the IP address assignment.
    The new VLAN IP address appears.
22. Return to the VLANs tab and repeat steps 10 through 13 to assign IP addresses to each additional VLAN.
23. Return to the VLANs table and enable routing for each of the newly configured VLANs by setting the routing value to **true**.

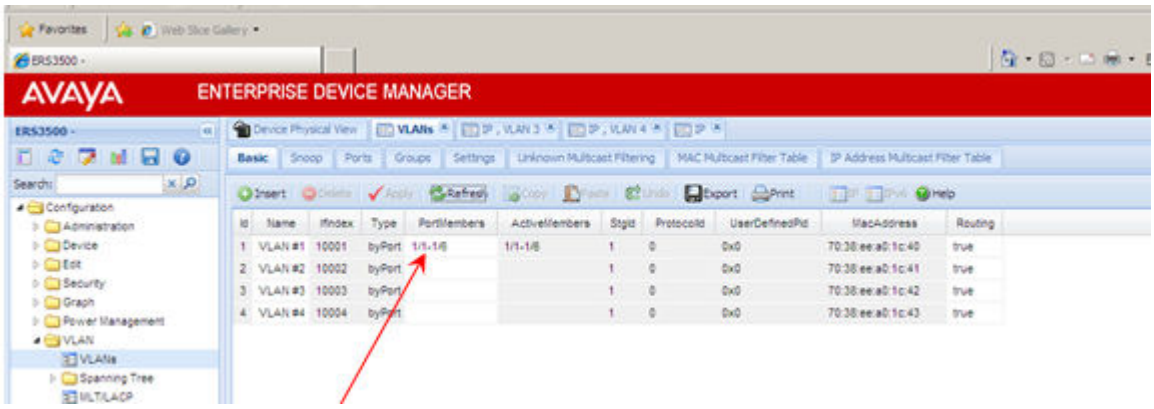
Note:

Perform the following steps to ensure that IP Routing has been enabled globally on the ERS.

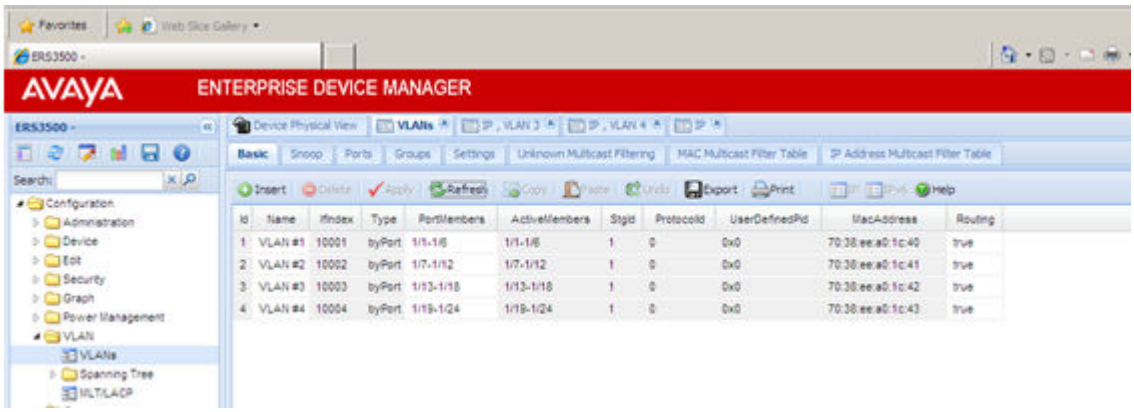
24. Navigate to the **IP** Folder.
25. Select **IP**.
26. Select the **Globals** tab.
27. Select the **forwarding** radio button.
28. Click apply.



29. From the VLANs tab, double-Click on the ports assigned to VLAN 1 and change to ports 1 – 6 .
30. Click **OK**.
31. Click **Apply**.
32. Click **Refresh**.



33. Repeat steps 22 through 25 to assign switch ports to the remaining VLANs as follows : VLAN 2 — Ports 7 – 12, V LAN 3 — Ports 13 – 18, and VLAN 4 — Ports 19 – 24.



34. Navigate to VLANs Settings tab and change VlanConfigControl to **autopvid**.
35. Modify VLANs 3 and 4 so that ports 13 – 24 are included in both VLANs .
36. Controlling traffic to and from the two VLAN assigned to ports 13 - 24.
37. Select the **Ports** tab.
38. Select Ports 13 - 24.
39. Set the default VLAN value.

    VLAN 4 is the Data VLAN
40. Select the tagging method of **untagPvidOnly** to send all untagged packets to the PC.

    When the phone receives packets from the network, it will forward all packets not belonging to VLAN 3 to the connected PC.

41. **Apply Selection**.
42. Click **Apply** .
43. Done