Getting Started with Avaya Ethernet Routing Switch 5000 Series

Release 6.6
NN47200-303
Issue 02.02
December 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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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 or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

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

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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”, or such successor site as designated by Avaya. 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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 or Hosted Service 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”). As required, 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 or such successor site as designated by Avaya. 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 or such successor site as designated by Avaya. 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, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides getting started concepts and procedures for the Avaya Ethernet Routing Switch 5000 Series. You can use the procedures in this document to connect and initially configure the switch for your network.

This document provides procedures for both the Avaya Command Line Interface (ACLI) and Enterprise Device Manager (EDM) for getting started tasks. You can access ACLI through either a direct console connection to the switch or by using the Telnet or SSH protocols to connect to the switch remotely. You can access EDM through a web browser to connect to the switch remotely.

The topics discussed in this document are provided with the following assumptions:

- You have a basic knowledge of networks, Ethernet bridging, and IP routing.
- You are familiar with networking concepts and terminology.
- You have basic knowledge of network topologies.
- You have experience with Graphical User Interface (GUI).
- You have experience with the following ACLI command modes:
  - User Executive
  - Privileged EXEC
  - Global configuration
  - Interface configuration

Related resources

Documentation

See the *Documentation Reference for Avaya Ethernet Routing Switch 5000 Series*, NN47200–103 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following sections indicate what is new in *Getting Started with Avaya Ethernet Routing Switch 5000 Series*, NN47200–303 for Release 6.6.

Features

See the following sections for information about feature changes.

ACLI show flash history command

The `show flash history` provides the current status of the Flash device. You can use the `show flash history` to view the flash writes and erase history on a standalone unit or stack. The Flash History does not record programming done from the diagnostics or bootloader. Flash History information is stored in the Serial (PC) Electrically Erasable Programmable Read Only Memory (SEEPROM). The data does not get corrupted during an upgrade or downgrade. Flash History is automatically enabled and does not require any configuration.

For more information on the `show flash` command, see

- Displaying flash information on page 123

.

Default IP

The Ethernet Routing Switch 5600 Series sets an IP address of 192.168.1.1/24 by default if the switch does not obtain its IP from another source.

For more information, see:

- Supported BootP modes on page 28

EDM improved download support

When downloading software to the switch, EDM provides a status bar on the progress and an indication when the download is complete.

For more information, see in this guide:

- Managing the configuration and image files on page 210

EDM inactivity timeout

You can configure the period of time that an EDM session remains idle before the session expires. The current default expiry for an idle EDM session is 15 minutes.

For more information, see:

- Configuring the EDM inactivity timeout on page 125

Out-of-band management

Out-of-band management allows switch or stack management through the dedicated out-of-band management port. This port can accept an IPv4 or IPv6 address different from the switch or stack IP address. With out-of-band management, you do not require an in-band management VLAN to carry switch or stack management traffic, including Telnet, Secure Shell (SSH) protocol, Simple Network Management Protocol (SNMP), HTTP, or HTTPS. You can also use out-of-band management to download a software image or access the Enterprise Device Manager (EDM) interface for a switch or stack.

For more information, see:

- Out-of-band management on page 36
- Configuring an out-of-band management IP address on page 46
- Configuring a management route on page 51
- Displaying out-of-band management information on page 49
- Enabling or disabling the out-of-band management port on page 50
- Configuring out-of-band management on page 166
- Configuring an out-of-band management IPv6 address on page 54
- Displaying out-of-band management IPv6 information on page 56

Run Scripts

You can use the run scripts to automatically configure the parameters for an Avaya Stackable Ethernet switch according to Avaya's best practices for converged solutions. The scripts can be executed in a default or verbose mode.

In the default mode, the switch is configured using predetermined parameter values. In the verbose mode, you can modify the default values and settings when the script is executed.

In this release, run scripts are available for IP Office, Link Layer Discovery Protocol (LLDP), and Auto Detect Auto Configuration (ADAC).

For more information, see

- Run Scripts on page 24

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 on page 113

.

VRF ping support

The ping command allows you to specify the VRF.

For more information, see in this guide:

- Using ping to test communication with another switch on page 68

Other changes

See the following sections for information about changes that are updates to previously existing information.

CLI interface change from FastEthernet to Ethernet

The CLI interface command `interface FastEthernet` is changed to `interface Ethernet`. The FastEthernet interface command remains available, but hidden so as to provide backward compatibility.

Dynamic management IP address change

You can dynamically change the in-band management IP address using Telnet, SSH, SNMP, HTTP, and HTTPS. For more information, see the following section in this guide:

- Configuring an in-band management IP address on page 43

In-band management

With the introduction of out-of-band switch or stack management, the previously existing IP management information is renamed to indicate in-band switch or stack management.

For more information, see the following sections in this guide:

- Configuring an in-band management IP address on page 43
- Obtaining an in-band management IP address automatically on page 45
- Setting in-band management IP address parameters from the ip.cfg file on a USB device on page 57

Removal of NSNA support

NSNA support has been removed for Avaya ERS 5600 Series starting in Release 6.6.

Chapter 3: Getting started fundamentals

Use the following sections to understand the feature concepts of the ERS 5000 Series and to get up and running quickly.

ACLI opening banner

The banner presented when a user logs in to the switch through ACLI can be configured to a user-defined value. The banner cannot exceed 1539 bytes, or 19 rows by 80 columns plus line termination characters.

When the system starts, the banner displays and prompts the user to enter `Ctrl+Y`. After these characters are entered, the system displays either a menu or the command line interface prompt, depending on previously configured defaults. To navigate between items in the menu, use the up/down arrow keys and select the item with the `Enter` key.

To switch the startup mode between menu and command line, see Setting the default management interface on page 41.

The banner control setting is saved to NVRAM, and both the banner file and control setting are distributed to all units within a stack.

To customize the opening banner, see Customizing the opening banner on page 120.

ACLI command modes

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, an out-of-band management port, 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
- Application Configuration
- Router Configuration

Mode access is determined by access permission levels and password protection.

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).

Application mode, also known as config-app mode, provides commands you can use to configure specific applications for the switch.

From the Global Configuration mode, access the Router Configuration Mode by entering one of the following commands:

- router rip
- router ospf
- router vrrp
- router bgp

Interface Configuration mode, also known as config-if 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 EXEC `5650TD-PWR>`	No entrance command, default mode	exit or logout
Privileged EXEC `5650TD-PWR#`	enable	exit or logout
Global Configuration `5650TD-PWR(config)#`	From Privileged EXEC mode, enter configure	To return to Privileged EXEC mode, enter: end or exit To exit ACLI completely, enter: logout
Interface Configuration `5650TD-PWR(config-if)#`	From Global Configuration mode, to configure a port, enter: interface Ethernet <port_number> To configure a VLAN, enter: interface vlan <vlan_number>	To return to Global Configuration mode, enter: exit To return to Privileged EXEC mode, enter: end To exit ACLI completely, enter: logout

Application Configuration
`5650TD-PWR(config-app)#`
	From Global Configuration mode: To enter application mode
	`application`
		To return to Global Configuration mode, enter
		`exit`
		To return to Privileged EXEC mode, enter
		`end`
		To exit ACLI completely, enter
		`logout`

Router Configuration `5650TD-PWR(config-router)#`	From Global Configuration mode: to configure OSPF, enter: router ospf To configure RIP, enter: router rip To configure VRRP, enter:	To return to Global Configuration mode, enter: exit To return to Privileged EXEC mode, enter: end

Command mode and sample prompt	Entrance commands	Exit commands
	router vrrp To configure BGP, enter: router bgp	To exit ACLI completely, enter: logout

See *Fundamentals of Avaya Ethernet Routing Switch 5000 Series*, NN47202-104 for more information about ACLI command modes.

User Access Limitations

ACLI enables the administrator to limit user access through the creation and maintenance of passwords for Telnet and Console access. This is a two-step process that requires first creating the password and then enabling it.

Ensure that **Global Configuration** mode is entered in ACLI before you begin these tasks.

Note:

When a username and password is set to default, the change is only applied to the unit on which the command was run.

Quick Start

You can use the **`install`** command in Avaya Command Line Interface (ACLI) or the Quick Start menu in Enterprise Device Manager (EDM) to configure the in-band IP Address and netmask, default gateway, read-only and read-write community strings, quick start VLAN,IPv6 in-band address, and IPv6 default gateway.

Configuring with Quick Start using ACLI

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

You must enter the following information when prompted:

- Quick start VLAN
- IP address

- Subnet mask
- Default gateway
- Read-only community string
- Read-write community string

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 5000 setup utility banner appears.
4. Enter the VLAN ID for the Quick Start at the following prompt:
   `Please provide the Quick Start VLAN <1-4094> [1]:`
5. Enter the IP address at the following prompt:
   `Please provide the in-band IP Address [0.0.0.0]:`
6. Enter the sub-net mask at the following prompt:
   `Please provide the in-band sub-net mask [255.255.255.0]:`
7. Enter the default gateway IP address at the following prompt:
   `Please provide the Default Gateway [0.0.0.0]:`
8. Enter the read only community string at the following prompt:
   `Please provide the Read-Only Community String [**********]:`
9. Enter the read write community string at the following prompt::
   `Please provide the Read-Write Community String [**********]:`
10. Enter the in-band IPv6 address at the following prompt:
    `Please provide the in-band IPV6 Address/Prefix_length [ : :/0]:`
11. Enter the in-band IPv6 default gateway at the following prompt:
    `Please provide the in-band IPV6 Default Gateway [ : :]:`

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

Example

```
################################################################################
         Welcome to the 5650TD-PWR setup utility.
You will be requested to provide the switch basic connectivity settings.
```

```
After entering the requested info, the configuration will be applied and
stored into the switch NVRAM.

Once the basic connectivity settings are applied, additional configuration
can be done using the available management interfaces.
Use Ctrl+C to abort the configuration at any time.

################################################################################

Please provide the Quick Start VLAN <1-4094> [1]:
Please provide the in-band IP Address[0.0.0.0]:
Please provide the in-band sub-net mask[255.255.255.0]:
Please provide the Default Gateway[0.0.0.0]:
Please provide the Read-Only Community String[**********]:
Please provide the Read-Write Community String[**********]:
Please provide the in-band IPV6 Address/Prefix_length[::/0]:
Please provide the in-band IPV6 Default Gateway[::]:


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

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

Run Scripts

You can use the run scripts to automatically configure the parameters for an Avaya Ethernet Routing switch according to Avaya's best practices for converged solutions.

The script executes a set of CLI commands in either a fully automated or user prompted configuration. In a fully automated or non-verbose mode, the scripts are executed with the predefined default values. In a user prompted or the verbose mode, the script allows you to modify the default values. Only the IP Office script can be executed in both default (non-verbose) and verbose mode. The LLDP and ADAC scripts run only in verbose mode.

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

Note:

Currently, only IPv4 configuration is supported.

The run script commands are only available from base unit. If you use the Telnet or SSH connection, you can lose the connection if the Management IP changes during the script execution.

In this release, run scripts are available for IP Office, Link Layer Discovery Protocol (LLDP), and Auto Detect Auto Configuration (ADAC).

Run IP Office script configuration

Use the Run IP Office script to configure parameters for the Ethernet Routing Switch 5600 according to Avaya best practices for converged solutions. You can execute the script in any of the two modes using ACLI or EDM:

- Non-verbose (default) mode — configures the switch using predetermined parameters
- Verbose mode — configures the switch using the parameters provided through ACLI prompts.

The configuration is optimized for solutions with Run IP Office that support a maximum of 250 users. You can quickly set up an ERS 5600 with Avaya IP Office.

The script sets VLAN IDs, IP addresses, QoS rules and tagging modes on switch ports to specific values, and sets PoE priorities for PWR units. The Link Layer Discovery Protocol (LLDP) for IP Phone detection is set automatically and switch ports are configured for the Run IP Office call server to connect.

Note:

The default subnet mask created by the Run IP Office script supports only 252 hosts. You can use the verbose mode to change the subnet mask to 255.255.254.0 to allow 508hosts for each subnet.

Table 1: Default parameters for Run IP Office 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
Data VLAN Gateway IP/mask	255.255.255.0
IP Route to Gateway Modem-Router (Internet/WAN)	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)	Gateway Modem-Router port

To use the IP Office script from ACLI, see Configuring with IP Office Script on page 84.

To configure IP Office script parameters using EDM, see Configuring with Run IP Office on page 170.

ADAC Script

The Run ADAC script optimizes the switch configuration for IP Telephony and Unified Communications solutions to support any number of users. The Run ADAC script saves time in configuring best practice configuration of the switching parameters in a setup where ADAC is used for detection and provisioning of IP Phones connected to an Avaya Ethernet switch or stack. Also, where LLDP is used for all configurations for voice communications over the data network.

The following configurations can be completed using the Run ADAC script:

- setting the port trust mode
- setting the DSCP values for Voice data and control plane (signalling)
- applying VLAN tagging modes on switch ports to specific values for accommodating tagged (IP Phone) and untagged VLAN (laptop or desktop PC device) behind the IP Phone

To use the ADAC script from ACLI, see Configuring with ADAC Script on page 86

To configure ADAC script parameters using EDM, see Configuring with Run ADAC on page 172.

LLDP Script

The Run LLDP script optimizes the switch configuration for IP Telephony and Unified Communications solutions to support any number of users. Run LLDP script saves time in configuring best practice configuration of the switching parameters in a setup where LLDP is used for detection and provisioning of IP Phones connected to an Avaya Ethernet switch or stack. Also, where LLDP is used for all configurations for voice communications over the data network.

The following configurations can be completed using the Run ADAC script:

- Setting the port trust mode.
- Setting the DSCP values for Voice data and control plane (signalling).
- Applying VLAN tagging modes on switch ports to specific values for accommodating tagged (IP Phone) and untagged VLAN (laptop or desktop PC device) behind the IP Phone.
- Setting call server and file server IP address to provision on the IP Phone.

To use the LLDP script from ACLI, see Configuring with LLDP Script on page 87.

To configure LLDP script parameters using EDM, see Configuring with Run LLDP on page 174.

Avaya Energy Saver

You can use Avaya Energy Saver (AES) to reduce network infrastructure power consumption without impacting network connectivity. AES uses intelligent switching capacity reduction in off-peak mode to reduce direct power consumption by up to 40%. AES can also use Power over Ethernet (PoE) port power priority levels to shut down low priority PoE ports and provide more power savings.

The power consumption savings of each switch is determined by the number of ports with AES enabled and by the power consumption of PoE ports that are powered off. If AES for a port is set to disabled, the port is not powered off, irrespective of the PoE configuration. AES turns off the power to a port only when PoE is enabled globally, the port AES is enabled, and the PoE priority for the port is configured to low.

You can schedule AES to enter lower power states during specified periods of time. These time periods can be a complete week, complete weekend, or individual days.

Avaya recommends disabling AES on uplink copper ports since activating or deactivating AES on copper ports will trigger a link down followed rapidly by a link up event. The best solution is to use fiber ports for uplinks since link status will not change when AES is activated or deactivated.

Important:

If a switch is reset while energy-saver is activated, the PoE power saving calculation may not accurately reflect the power saving, and in some cases may display zero savings. This is because the switch did not have sufficient time to record PoE usage between the reset of the switch and energy-saver being reactivated. When energy saver is next activated, the PoE power saving calculation will be correctly updated.

Boot agent image

The Dual Agent feature provides support for two agents for Ethernet Routing Switch 5600 series in stand-alone or stack configuration.

The Dual Agent feature provides two agent images, the Agent Primary image and the Agent Secondary image. The Agent Primary image represents the agent image used for the next boot. You are able to select either image for the next boot.

The Dual Agent Boot flag determines which agent image is the boot image. The diagnostics and agent software must use the same value for the Dual Agent Boot flag.

If the Dual Agent Boot flag is not set, the unit will boot from Agent 1 (default).

Supported BootP modes

The Avaya Ethernet Routing Switch 5600 Series supports the Bootstrap protocol (BootP).

BootP enables you to retrieve an ASCII configuration file name and configuration server address.

A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask and the IP address of the default router (default gateway).

The Avaya Ethernet Routing Switch 5600 Series has a unique 48-bit hardware address, or MAC address, that is printed on a label on the back panel. Use this MAC address when you configure the network BootP server to recognize the Avaya Ethernet Routing Switch 5600 Series BootP requests.

The supported BootP modes are:

- BootP or Default IP (default mode)
- BootP Always
- BootP Disabled
- BootP or Last Address

BootP or Default IP

The Ethernet Routing Switch 5600 Series operates in the BootP or Default IP mode (the default mode) as follows:

- After the switch is reset or power cycled, if the switch has a configured IP address other than 0.0.0.0 or the default IP address, then the switch uses the 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 5600 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 5600 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 5600 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).

Asset ID configuration

You can define an Asset ID to provide inventory information for the switch, stack, or each unit in a stack. An Asset ID consists of an alphanumeric string of up to 32 characters in length. An Asset ID is useful for recording your company specific asset tracking information, such as an asset tag attached to the unit.

Simple Network Time Protocol

The Simple Network Time Protocol (SNTP) is a subset of the Network Time Protocol. It provides a simple mechanism for time synchronization. NTP enables clocks to be synchronized to a few milliseconds, depending on the clock source and local clock hardware.

SNTP synchronizes to the Universal Coordinated Time (UTC) with an error of less than one second. This feature adheres to the RFC 2030 (MIB is the s5agent). With this feature, the system can obtain the time from any RFC 2030-compliant NTP or SNTP server.

SNTP accuracy is typically in the order of "significant fractions of a second." This accuracy is related to the latencies between the SNTP client device and the NTP server. In a low latency network, the SNTP accuracy can be reduced to the sub-100 millisecond range and, to further increase the accuracy, a simple latency measurement algorithm can be used. The intended accuracy for this implementation is one second, which is sufficient for logs and time displays on user interfaces.

The SNTP feature allows you to set an offset from GMT for the time zone of your location. You can also set a start date and end date and offset for Daylight Savings Time.

The SNTP client implementation for this feature is unicast. The SNTP client operates typically in a unicast mode, but also can use the broadcast and multicast modes.

When SNTP is enabled (the default state is disabled), the system synchronizes with the configured NTP server at bootup (after network connectivity is established) and at user-configurable periods thereafter (the default synchronization interval is 24 hours). The synchronization also can happen upon manual request.

The SNTP feature supports both primary and secondary NTP servers. SNTP attempts to contact the secondary NTP server only if the primary NTP server is unresponsive. When a server connection fails, SNTP retries for a maximum of three times, with five minutes between each retry.

Auto-MDI X

The term auto-MDI/X refers to automatic detection of transmit and receive twisted pairs.

Auto-MDI/X detects, receive, and transmit twisted pairs automatically. When auto-MDI/X is active, any straight or crossover category 5 cable can be used to provide connection to a port. If autonegotiation is disabled, then auto-MDI/X is not active.

Auto-polarity

The term auto-polarity refers to the ability of the port to compensate for positive and negative signals being reversed on the receive cables.

The Avaya Ethernet Routing Switch 5000 Series support auto-polarity. With autonegotiation enabled, auto-polarity automatically reverses the polarity of a pair of pins from positive to negative or negative to positive. This corrects the polarity of the received data, if the port detects that the polarity of the data has been reversed due to a wiring error. If autonegotiation is disabled, auto-polarity is not active.

Autosensing and autonegotiation

The Avaya Ethernet Routing Switch 5000 Series are autosensing and autonegotiating devices:

- 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 or 802.3z or 802.3ab) that exists between two IEEE-capable devices. Autonegotiation enables the switch to select the best 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 802.3z autonegotiation standard. If it is not possible to sense the duplex mode of the attached device, the Avaya Ethernet Routing Switch 5000 Series reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the Avaya Ethernet Routing Switch 5000 Series, the ports negotiate down from 1000 Mbps speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

Secure File Transfer Protocol

You can use one of two distinct software images for the ERS 5000 Series switch. The secure software image supports the Secure Shell (SSH) network protocol while the standard software image does not include SSH functionality. SSH can replace telnet to provide secure access to the user console menu and ACLI interface. Avaya Ethernet Routing Switches use SSH version 2 for secure remote logon and other secure network services over an insecure network.

For switches running a secure software image, with Secure Shell (SSH) enabled, you can enhance network security by using Secure File Transfer Protocol (SFTP) to transfer files between a switch or stack and an SFTP server that supports SFTP with Secure Shell (SSH) version 2.

SFTP is enabled by default and interacts with SSH client.

To enhance network security, you can use SFTP to transfer files between a switch or stack and an SFTP server. With SFTP over SSH, you can perform the following file transfers with a higher level of security than basic SFTP:

The switch supports the following SFTP functions:

- uploading binary configuration files to an SFTP server
- downloading binary configuration files from an SFTP server
- uploading ASCII configuration files to an SFTP server
- downloading ASCII configuration files from an SFTP server
- downloading agent software from an SFTP server
- downloading of diagnostics software from an SFTP server
- downloading of license files from an SFTP server
- DHCP external save transfer to and from an SFTP server
- DSA-key authentication support
- RSA-key authentication support
- password authentication support
- host key generation support
- 1024-bit DSA-key use for authentication
- support for the configuration of SFTP address independent of TFTP server address

For more information about SSH, see *Configuring Security on Avaya Ethernet Routing Switch 5000 Series*, NN47200-501.

Auto Unit Replacement (AUR)

You can use the Auto Unit Replacement (AUR) feature 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. Stack power must be on during the procedure because CFG mirror images are retained in the DRAM of the stack.

Important:

For Auto Unit Replacement to function properly, the new unit and the existing units in the stack must all run the same version of software and diagnostic. In case of a two unit stack, only replacing a non-base unit is currently supported.

You can manually restore an associated configuration (same unit number) of a unit in a stack including base unit (if the stack is of 3 units or bigger).

Important:

If the base unit is reset before you restore the configuration, the base unit erases the saved configuration information for non-base units.

The following information also relates 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 configuration is overwritten with the restored configuration from the stack.
- You can enable or disable this feature at any time. The default mode is ENABLE.
- Customer log messages are provided.

Important:

After booting 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 duplicate CFG image (stored in non-volatile memory) 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 is 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.

The CFG mirror image process is triggered by the following specific events:

- Power cycle
- Adding a unit
- Removing a unit
- Restoring a CFG image
- Synchronizing the CFG mirror images with CFG images

Removing a MAC address from the AUR cache

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.

Note:

You can remove a MAC address from the AUR cache to perform an AUR without replacing the physical unit.

Agent Auto Unit Replacement (AAUR)

Agent Auto Unit Replacement (AAUR) is an AUR enhancement to ensure that all units in a stack have the same software image. AAUR inspects units joining a stack and downloads the agent software image to any unit that has a dissimilar image. AAUR is enabled by default.

When you add a unit, AAUR functions in the following manner:

1. The added unit runs in stand-alone mode and AAUR inspects the added unit agent software image.
2. If the added unit agent image differs from the stack agent image, AAUR transfers the stack agent image to the added unit.

- The added unit sends an AAUR request to the cascade up port. If the added unit does not receive an answer, it sends an AAUR request to the cascade down port.

3. The added unit resets, and completes adjacency to the stack upon a reboot.

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

```
I 2 00:01:56:40 13 AAUR - Info: Receive request for agent image, start transfer
I 2 00:01:56:48 14 AAUR - Info: Agent transfer finished
```

Stack Forced Mode

Stack Forced Mode allows one or both units to become stand-alone switches if a stack of two units fails. With Stack Forced Mode, you can manage one of the stand-alone devices from a failed stack of two with the previous stack IP address.

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, gateway), and an administrator can reach the device by Telnet or EDM, through an IP connection.

If you enable Stack Forced Mode on a stack, you enable Stack Forced Mode on all units in the stack. Stack Forced Mode becomes active only if the stack of two fails. When 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.

When a failure occurs on a Stack Forced Mode stack of two units, the previous non-base unit sends out a gratuitous ARP onto the management network. The gratuitous ARP is sent to determine if the base unit is still operational and using the stack IP address. A failure situation in which both the base unit and non-base unit remain operational, but not part of a stack could be possible if the stack cable is removed or failed. If the previous non-base unit receives a reply from the previous base unit of the stack, the previous non-base unit does not take over ownership of the stack IP address, and uses the local switch IP address if configured. If the previous non-base unit does not receive a response from the previous base-unit, the previous non-base unit takes over ownership of the stack IP address and issues a gratuitous ARP with its own MAC address to ensure that all devices on the management VLAN update their ARP caches appropriately.

Stack Forced Mode allows non-EAP clients connected to the device to still authenticate themselves and maintain connectivity to the network. 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 remains in Stack Forced Mode until a reboot or until it joins a stack.

A settlement timer prevents a unit from entering Stack Forced Mode if several stack failures occur within a few seconds, or if a stack is larger than two units. A unit can enter Stack Forced Mode only if it is joined to a stack of two units for 30 seconds or longer.

If the switch is in Stack Forced Mode and you want to configure an IPv6 address, you must first delete the active IPv6 interface and then configure the switch IPv6 address. If you use Telnet, SSH or EDM to change the settings, you can lose IPv6 connectivity to the switch. Avaya recommends that you change the settings with the Console Interface, or use an IPv4 address for management.

IP blocking

Along with IP Routing, you can use Blocking Mode in two modes: full and none. The following paragraphs show how blocking mode acts for a stack.

You have a stack with IP Routing enabled and some Layer 3 VLANs. Assign VLANs ports from all the units. Set IP blocking-mode to Full on the base unit. Remove all the units from stack. All of the units will run in Layer 2 mode. No Layer 3 settings will be available on these units.

You have a stack with IP Routing enabled, and some Layer 3 VLANs. Assign VLANs ports from all the units. Set the IP blocking-mode to None on the base unit. Remove all of the units from stack. The Layer 3 settings made on the stack will be available on these units. By default IP blocking-mode is None.

Out-of-band management

Out-of-band management allows IPv4 or IPv6 switch or stack management using the dedicated out-of-band management port. Out-of-band management supports Telnet, Secure Shell (SSH) protocol, Simple Network Management Protocol (SNMP), HTTP, or HTTPS, without requiring an in-band management VLAN.

To configure out-of-band management, you assign an IP address to the RJ-45 Ethernet management port for a switch or stack. You can configure a specific out-of-band management default gateway, which takes precedence over the in-band default gateway. If you do not configure an out-of-band management default gateway, the in-band default gateway is used for out-of-band switch or stack management.

Note:

The out-of-band switch or stack management IP address must be different than the in-band IP address and belong to a different subnet.

You can use the out-of-band management port to perform tasks such as downloading software images and, when the SNMP server is enabled, access the Enterprise Device Manager (EDM) interface for a switch or stack. To access EDM, you type the out-of-band management IP address in the address bar of an Internet browser.

The out-of-band management port supports full auto negotiation, which enables management stations to connect at any of the supported speeds or duplexes.

Considerations and limitations

The following considerations and limitations apply when you configure and use out-of-band management:

- You must configure all out-of-band management IP addresses for a stack to the same subnet.
- You can configure only one out-of-band management default gateway for each stack.
- You cannot automatically obtain an out-of-band management IP address using BootP or DHCP.
- With out-of-band management you can issue the **`ping`** command from the out-of-band management port on a stack base unit only.
- With out-of-band management you can only download a software image, or load a configuration file from the base unit in a stack.
- You can access a management stack from the out-of-band management port on the stack base unit only.
- You can configure both an in-band and out-of-band management IP:
  - The out-of-band management default gateway takes precedence over the in-band management default gateway.
  - In Layer 2 mode, once an out-of-band management default gateway is configured, the in-band management address is reachable only through a directly attached subnet for the management VLAN.
  - In Layer 3 mode, you must configure a management route to maintain connectivity with the management network when you use out-of-band management.
- The MAC address for the out-of-band management port is created using the switch MAC address plus the management offset. The management offset value for the primary out-of-band management port is 0x300 and the management offset value for the secondary out-of-band management port is 0x301..
- The out-of-band management port speed is automatically negotiated, however, you can change it manually.

- The out-of-band management port does not support generation or processing of Autotopology packets when an out-of-band management IP is configured.
- RADIUS authentication is not supported for the out-of-band management IP.

Chapter 4: Connecting to the switch

Connecting a terminal to the switch

Use this procedure to connect a terminal to the console port on the switch.

Before you begin

- Terminal with AC power cord and keyboard. Refer to *Quick Installation of Avaya Ethernet Routing Switch 5000 Series*, NN47200–105 for terminal emulation settings.
- RJ45 serial cable. The maximum length for the console port cable is 25 feet (8.3 meters).

Refer to *Installing the Avaya Ethernet Routing Switch 5000 Series*, NN47200-300 for console port in-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 serial cable to the connector on the terminal.
2. Connect the other end of the serial cable to the console port on the switch.
3. Turn the terminal on.
4. Set the terminal protocol on the terminal or terminal emulation program to VT100 and 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.

```
********************************************************************************
***********
         Welcom to the 5650TD 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 itnerfaces.
Use Ctrl+C to abort the configuration at any time.
```

```
**********************************************************************
**********

Please provide the Quick Start VLAN <1-4094? [1]:
Please provide the in-band IP Address[192.168.1.1]:
Please provide the in-band sub-net mask[255.255.255.0]:
Please provide the Default Gateway[0.0.0.0]:
Please provide the management sub-net mask[0.0.0.0]:
Please provide the management IP Address[0.0.0.0]:
Please provide the management Default Gateway[0.0.0.0]:
Please provide the Read-Only Community String[public]:
Please provide the Read-Write Community String[private]:
Please provide the in-band IPV6 Address/Prefix_length[::/0]:
Please provide the in-band IPV6 Default Gateway[::]:
Please provide the management IPV6 Address/Prefix_length[::/0]:
Please provide the management IPV6 Default Gateway[::]:

**********************************************************************
**********
Basic switch 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.

Note:

The **`show terminal`** command can be used at any time to display the current terminal settings. This command takes no parameters.

Procedure

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

   ```
   terminal speed {2400|4800|9600|19200|38400} length <0-132>
   width <1-132>
   ```

Variable definitions

The following table outlines the parameters of the **terminal** command.

Variable	Value
speed {2400|4800| 9600|19200| 38400}	Sets the transmit and receive baud rates for the terminal. The speed can be set at one of the five options shown. DEFAULT: 9600
length	Sets the length of the terminal display in lines. DEFAULT: 23 **Note:** If the terminal length is set to a value of 0, the pagination is disabled and the display continues to scroll without stopping.
width	Sets the width of the terminal display in characters. DEFAULT: 79

Setting the default management interface

Use this procedure to set the default management interface.

About this task

You can set the default management interface with ACLI to suit the preferences of the switch administrator. This selection is stored in NVRAM and propagated to all units in a stack configuration. When the system is started, the banner displays and prompts the user to enter `Ctrl+Y`. After these characters are entered, the system displays either a menu or the command line interface prompt, depending on previously configured defaults. When using the console port, you must log out for the new mode to display. When using Telnet, all subsequent Telnet sessions display the selection.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. To set the default management interface to display a menu, enter the following command:

   ```
   cmd-interface menu
   ```

3. To set the default management interface to display a command line interface prompt, enter the following command:

   ```
   cmd-interface cli
   ```

Chapter 5: Configuring management IP addresses using ACLI

This chapter provides procedural information you can use to assign, clear, and view in-band and out-of-band management IP addresses and gateway IP addresses.

Configuring an in-band management IP address

Use this procedure to configure the in-band management IPv4 address, subnet mask, and default gateway for a switch or stack.

Important:

Changing or clearing the in-band management IP address or subnet mask disconnects any active IP management connections.

About this task

You can dynamically change the in-band management IP address using Telnet, SSH, SNMP, HTTP, and HTTPS.

Procedure

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. To assign or modify the in-band management IP address for a switch or stack, enter the following at the command prompt:
   ```
   ip address [switch | stack | unit <1-8>] <A.B.C.D> [netmask <A.B.C.D>] [default-gateway <A.B.C.D>]
   ```

   Note:

   You configure the stack in-band management IP address on the stack base unit.

   Important:

   Only one management default gateway can operate for each unit or stack. The out-of-band management default gateway takes precedence over the in-band

management default gateway. Once an out-of-band management default gateway is configured, the in-band management address is reachable only through a directly attached subnet for the management VLAN.

3. To clear the in-band management IP address and the default gateway, enter the following commands at the command prompt:

```
no ip address [switch | stack | unit <1-8>]
no ip default-gateway
```

Example

```
5650TD-PWR>enable
5650TD-PWR#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
5650TD-PWR(config)#ip address stack 172.16.1.80 netmask 255.255.255.0 default-
gateway 172.16.1.1
5650TD-PWR(config)#ip address switch 172.16.1.81
5650TD-PWR(config)#ip address unit 2 172.16.1.82
5650TD-PWR(config)#ip address unit 3 172.16.1.83
```

Variable definitions

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

Variable	Value
switch	Specifies an in-band management IP address for an individual switch (standalone or stack unit).
stack	Specifies an in-band management IP address for the stack.
unit <*1–8*>	Specifies an in-band management IP address for a specific stack unit. Values range from 1–8.
<A.B.C.D>	Specifies an in-band management IPv4 address.
netmask <*A.B.C.D*>	Specifies the subnet mask associated with the in-band management IP address for a standalone switch or for a specific switch unit within a stack. **Note:** Although netmask appears as an optional parameter with the **`ip address`** command, Avaya recommends that you change the netmask when you dynamically change the in-band

Variable	Value
	management IP address for a switch or stack.
default-gateway <*A.B.C.D*>	Specifies the default gateway IP address.

Note:

If you do not specify a parameter with the **`ip address`** command, the system automatically modifies the stack IP address when in stack mode, and modifies the switch IP address when in standalone mode.

Obtaining an in-band management IP address automatically

Use this procedure to automatically obtain an in-band management IP address, subnet mask and default gateway on the switch or stack.

About this task

When you use DHCP, the switch or stack can also obtain up to three DNS server IP addresses.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   ip address source {bootp-always | bootp-last-address | bootp-when-needed | configured-address | dhcp-always | dhcp-last-address | dhcp-when-needed}
   ```

Variable definitions

The following table describes the parameters for the **`ip address source`** command.

Variable	Value
bootp-always	Always use the BootP server.

Variable	Value
bootp-last-address	Use the last BootP server.
bootp-when-needed	Use the BootP server when needed. DEFAULT: bootp-when-needed
configured-address	Use the manually configured IP configuration.
dhcp-always	Always use the DHCP server.
dhcp-last-address	Use the last DHCP server.
dhcp-when-needed	Use DHCP client when needed.

Displaying in-band management information

Use this procedure to display the stack and switch in-band management IP addresses, BootP/DHCP mode, stack address, switch address, subnet mask, and the in-band default-gateway IP address.

About this task

This command displays the parameters for what is configured, what is in use, and the last BootP/DHCP. If you do not enter any parameters, this command displays all IP-related configuration information.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:
   ```
   show ip [address] [address source] [bootp] [default-gateway]
   ```

Configuring an out-of-band management IP address

Use this procedure to configure the out-of-band management IPv4 address, subnet mask, and default gateway for a switch or stack.

Before you begin

You must connect the RJ-45 cable for link-up in out-of-band management mode to rear-port A.

About this task

When you physically connect the Ethernet RJ-45 out-of-band management port for a standalone switch or stack to your network, and assign an IPv4 address and subnet to the port,

you can use out-of-band management to access the switch or stack using Telnet, SSH, SNMP, HTTP, and HTTPS.

Note:

The out-of-band management IP address must be different than the switch or stack in-band management IP address and must belong to a different subnet.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To assign or modify an out-of-band management IP address for a switch or stack, enter the following command at the command prompt:

   ```
   ip mgmt {[address [switch | stack | unit <1-8>] <A.B.C.D>] |
   [netmask <A.B.C.D>] | [default-gateway <A.B.C.D>] }
   ```

   Note:

   You must configure the stack out-of-band management IP address on the base unit.

   Important:

   Only one management default gateway can operate for each unit or stack. The out-of-band management default gateway takes precedence over the in-band management default gateway. Once an out-of-band management default gateway is configured, the in-band management address is reachable only through a directly attached subnet for the management VLAN.

3. To clear the out-of-band management IP address for a switch or stack, enter the following command at the command prompt:

   ```
   no ip mgmt address [switch | stack]
   ```

4. To clear the out-of-band management default gateway, enter the following command at the command prompt:

   ```
   no ip mgmt default-gateway
   ```

Example

```
5650TD-PWR>enable
5650TD-PWR#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
5650TD-PWR(config)#ip mgmt address stack 172.16.100.80 netmask 255.255.255.0
5650TD-PWR(config)#ip mgmt address unit 1 172.16.100.81 netmask 255.255.255.0
5650TD-PWR(config)#ip mgmt address unit 2 172.16.100.82 netmask 255.255.255.0
5650TD-PWR(config)#ip mgmt address unit 3 172.16.100.83 netmask 255.255.255.0
```

Variable definitions

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

Variable	Value
switch	Specifies an out-of-band management IP address for an individual switch (standalone or stack unit).
stack	Specifies an out-of-band management IP address for the stack.
unit <*1–8*>	Specifies an out-of-band management IP address for a specific stack unit. Values range from 1 to 8. **Note:** The unit parameter is available only in a stack environment.
<*A.B.C.D*>	Specifies an out-of-band management IPv4 address. DEFAULT: 0.0.0.0
netmask <*A.B.C.D*>	Specifies the subnet mask associated with the out-of-band management IP address. DEFAULT: 0.0.0.0 **Note:** Although netmask appears as an optional parameter with the **ip mgmt address** command, Avaya recommends that you change the netmask when you dynamically change the out-of-band management IP address for a switch or stack.
default-gateway <*A.B.C.D*>	Specifies the management default gateway. Only specify an out-of-band default gateway if you are not routing the management IP.
Important: The out-of-band management IP addresses for all stack units must belong to the same subnet.	

Displaying out-of-band management information

Use this procedure to display out-of-band management configuration information for a switch or stack.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. At the command prompt, enter the following command:
   ```
   show ip mgmt [all | route]
   ```

Example

```
5650TD-PWR>show ip mgmt all

Unit  Ip Address      Netmask         Gateway         Link / Speed  Status
----- --------------- --------------- --------------- ------------- ---------
Stack 149.4.5.178     255.255.255.240 149.4.5.177     Up 1000F            Enabled
1     149.4.5.179     255.255.255.240 149.4.5.177     Up 1000F            Enabled
2     149.4.5.180     255.255.255.240 149.4.5.177     Up 1000F            Enabled
```

Note:
In a stack environment, the base unit is identified as Stack in the Unit column.

Variable definitions

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

Variable	Value
all	Displays out-of-band management configuration information for all units within a stack.
route	Displays management VLAN information.

Note:
If you do not enter a variable with the **`show ip mgmt`** command, out-of-band management configuration information for the local switch is displayed.

Enabling or disabling the out-of-band management port

Use this procedure to administratively enable or disable the Ethernet RJ-45 out-of-band management port.

Procedure

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. To disable the out-of-band management port, enter the following command at the command prompt:
   ```
   ip mgmt shutdown [all | unit <1-8>]
   ```
3. To enable the out-of-band management port, enter the following command at the command prompt:
   ```
   no ip mgmt shutdown [all | unit <1-8>]
   ```

Result

After you use the **`no ip mgmt shutdown [all | unit <1-8>]`** command to enable an out-of-band management port, there is a delay of approximately 90 seconds before the port is reachable.

Variable definitions

The following table describes the parameters for the **`ip mgmt shutdown`** and **`no ip mgmt shutdown`** commands.

Variable	Value
all	Specifies to enable or disable the management port of all units in a stack.
unit *<1–8>*	Specifies a specific switch unit within a stack for which to enable or disable the out-of-band management port.

Configuring a management route

Use this procedure to configure a management route. In Layer 3 mode, If you configure management routes you can access both the out-of-band and in-band management addresses.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To assign an IP management route, enter the following command at the command prompt:

   ```
   ip mgmt route <destination-IP> <destination-netmask>
   <destination-gateway>
   ```

3. To clear an IP management route, enter the following command at the command prompt:

   ```
   no ip mgmt route <destination-IP> <destination-netmask>
   <destination-gateway>
   ```

Variable definitions

The following table describes the parameters for the **`ip mgmt route`** command.

Variable	Value
<destination-IP>	Specifies the destination IPv4 address.
<destination-netmask>	Specifies the destination IPv4 subnet mask.
<destination-gateway>	Specifies the destination IPv4 gateway.

Configuring an in-band management IPv6 address

Use this procedure to configure the in-band management IPv6 address for a switch or stack.

Important:

Changing or clearing the in-band management IPv6 address disconnects any active IP management connections.

About this task

You can dynamically change the in-band management IPv6 address using Telnet, SSH, SNMP, HTTP, and HTTPS.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To assign or modify the in-band management IPv6 address for a switch or stack, enter the following at the command prompt:

   ```
   ipv6 address [switch | stack | unit <1-8>] <WORD>
   ```

   Note:

   You configure the stack in-band management IPv6 address on the stack base unit.

   Important:

   Only one management default gateway can operate for each unit or stack. The out-of-band management default gateway takes precedence over the in-band management default gateway. Once an out-of-band management default gateway is configured, the in-band management address is reachable only through a directly attached subnet for the management VLAN.

3. To assign the default gateway, enter the following at the command prompt:

   ```
   ipv6 default-gateway <WORD>
   ```

4. To clear the in-band management IPv6 address and the default gateway, enter the following commands at the command prompt:

   ```
   no ipv6 address [switch | stack | unit <1-8>]
   no ipv6 defaul-gateway
   ```

Example

```
5650TD-PWR>enable
5650TD-PWR#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
5650TD-PWR(config)#ipv6 address stack 2005::2/64
5650TD-PWR(config)#ipv6 default gateway 2005::1
5650TD-PWR(config)#ipv6 address switch 2005::3
5650TD-PWR(config)#ipv6 address unit 2 2005::4
5650TD-PWR(config)#ipv6 address unit 3 2005::5
```

Variable definitions

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

Variable	Value
switch	Specifies an in-band management IPv6 address for an individual switch (standalone or stack unit).
stack	Specifies an in-band management IPv6 address for the stack.
unit <*1–8*>	Specifies an in-band management IPv6 address for a specific stack unit. Values range from 1–8.
<WORD>	Specifies an in-band management IPv6 address.
default-gateway <*WORD*>	Specifies the default gateway IPv6 address.

Note:

If you do not specify a parameter with the **ipv6 address** command, the system automatically modifies the stack IPv6 address when in stack mode, and modifies the switch IPv6 address when in standalone mode.

Displaying in-band IPv6 management information

Use this procedure to display the stack and switch in-band management IPv6 addresses, and the in-band default-gateway IPv6 address.

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display the configured in-bank management IPv6 address, enter the following at the command prompt:

   ```
   show ipv6 address [stack][switch][unit <1-8>]
   ```

3. To display IPv6 default-gateway information, enter the following at the command prompt:

```
show ipv6 default-gateway
```

Example

```
5650TD-PWR>show ipv6 address

Switch Address: 2005::2/64
Stack Address:  2005::2/64

5650TD-PWR>show ipv6 default-gateway

Default Gateway: 2005::1
Status: NotActive
```

Note:

The status of the default gateway is active when the IPv6 address configured is reachable.

Configuring an out-of-band management IPv6 address

Use this procedure to configure the out-of-band management IPv6 address and default gateway for a switch or stack.

About this task

When you physically connect the Ethernet RJ-45 out-of-band management port for a standalone switch or stack to your network, and assign an IPv6 address and subnet to the port, you can use out-of-band management to access the switch or stack using Telnet, SSH, SNMP, HTTP, and HTTPS.

Note:

In Layer 3 mode, both interfaces of the switch are reachable if the routes are configured. If you are initiating the connection from the switch interfaces (serial, Telnet, SSH), the out-of-band management route takes precedence. For example, if you execute a traceroute to a distant host, the out-of-band route is chosen.

Note:

The out-of-band management IP address must be different than the switch or stack in-band management IP address and must belong to a different subnet.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To activate the IPv6 interface on the switch, enter the following command at the command prompt:

   ```
   ipv6 mgmt interface
   ```

3. To assign or modify an out-of-band management IPv6 address for a switch, stack or unit, enter the following command at the command prompt:

   ```
   ipv6 mgmt { [address [switch | stack | unit <1-8>] <WORD>] |
   default-gateway <WORD> }
   ```

   Note:

   You must configure the stack out-of-band management IPv6 address on the base unit.

   Important:

   Only one management default gateway can operate for each unit or stack. The out-of-band management default gateway takes precedence over the in-band management default gateway. Once an out-of-band management default gateway is configured, the in-band management address is reachable only through a directly attached subnet for the management VLAN.

4. To clear the out-of-band management IPv6 address for a switch, stack, or unit, enter the following command at the command prompt:

   ```
   no ipv6 mgmt address [switch | stack | unit <1-8>]
   ```

5. To clear the out-of-band IPv6 management default gateway, enter the following command at the command prompt:

   ```
   no ipv6 mgmt default-gateway
   ```

Example

```
5650TD-PWR>enable
5650TD-PWR#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
5650TD-PWR(config)#ipv6 mgmt address stack 4149:4:4:360::2/59
% IPV6 Oob management interface does not exist
5650TD-PWR(config)#ipv6 mgmt interface
5650TD-PWR(config)#ipv6 mgmt address stack 4149:4:4:360::2/59
5650TD-PWR(config)#show ipv6 mgmt interface
2013-08-06 17:28:49 GMT+02:00    UTC time: 2013-08-06 15:28:49
================================================================================
                 Interface Information
 ================================================================================
IFINDX VLAN-ID  MTU  PHYSICAL          ADMIN    OPER  RCHBLE  RETRAN  TYPE
ADDRESS           STATE    STATE TIME    TIME
--------------------------------------------------------------------------------
55001  1        1500 00:19:e1:55:07:00 enabled  up    30000   1000    ETHER
================================================================================
                 Address Information
================================================================================
INTF   IPV6                                  TYPE    ORIGIN    STATUS INDEX  ADDRESS
--------------------------------------------------------------------------------
55001  4149:4:4:360::2                         UNICAST MANUAL    PREFERRED
55001  fe80::219:e1ff:fe55:700                 UNICAST LINKLAYER PREFERRED
```

```
1 out of 1 Total Num of Interface Entries displayed.

2 out of 8 Total Num of Address Entries displayed.
```

Displaying out-of-band management IPV6 information

Procedure

1. Log on to ACLI to enter User EXEC mode.
2. To display all addresses for IPv6 interfaces, enter the following command at the command prompt:
   ```
   show ipv6 address interfaces
   ```
3. To display IPv6 management addresses, enter the following command at the command prompt:
   ```
   show ipv6 mgmt address [unit <1-8>]
   ```
4. To display IPv6 management default-gateway information, enter the following command at the command prompt:
   ```
   show ipv6 mgmt default-gateway
   ```
5. To display IPv6 management interface information, enter the following command at the command prompt:
   ```
   show ipv6 mgmt interface
   ```
6. To display the neighbor table for the IPv6 management port, enter the following command at the command prompt:
   ```
   show ipv6 neighbor interface mgmt
   ```
7. To display the routing table for the IPv6 management port, enter the following command at the command prompt:
   ```
   show ipv6 route mgmt
   ```

Example

```
5632FD(config)#show ipv6 mgmt address
2013-08-06 17:32:00 GMT+02:00    UTC time: 2013-08-06 15:32:00

Mgmt Switch Address: ::/0
Mgmt Stack Address:  4149:4:4:360::2/59
```

```
5632FD(config)#show ipv6 neighbor interface mgmt
2013-08-06 17:32:45 GMT+02:00    UTC time: 2013-08-06 15:32:45
================================================================================
                  Neighbor Information
================================================================================
NET ADDRESS/                                PHYS   TYPE    STATE      LAST
PHYSICAL ADDRESS                            INTF                      UPD
--------------------------------------------------------------------------------
4149:4:4:360::/                             O-1    LOCAL   REACHABLE  0
```

```
00:19:e1:55:07:00
4149:4:4:360::1/                                O-1    DYNAMIC REACHABLE  17061
00:19:e1:4d:7c:9c
4149:4:4:360::2/                                O-1    LOCAL   REACHABLE  16847
00:19:e1:55:07:00
fe80::219:e1ff:fe55:700/                        O-1    LOCAL   REACHABLE  16847
00:19:e1:55:07:00

 4 out of 13 Total Num of Neighbor Entries displayed.
```

Setting in-band management IP address parameters from the ip.cfg file on a USB device

If the switch does not obtain an in-band management IP address through BootP, you can load the IP address and optionally new switch software and configuration from the USB memory device using the `ip.cfg` file.

Note:

The file name, `ip.cfg`, is case-insensitive.

If a properly formatted file exists on a USB port, the switch uses that `ip.cfg` as the first option, rather than the last. You can specify one or more of the optional parameters in the `ip.cfg` file. All of the parameters are optional.

The following table describes the `ip.cfg` file parameters:

Parameter	Description
IP <*A.B.C.D*> | <*WORD*>	Specifies the IP address for the switch. A.B.C.D is IPv4 address, WORD is IPv6 address.
Mask <*xx.xx.xx.xx*>	Specifies the IPv4 network mask. Example: 255.255.255.0
Gateway <*A.B.C.D*> | <*WORD*>	Specifies the default gateway. A.B.C.D is IPv4 address, WORD is IPv6 address.
SNMPread <*string*>	Specifies the SNMP read community string. Example: public
SNMPwrite <*string*>	Specifies the SNMP write community string. Example: private
VLAN <*number*>	Specifies the management VLAN-ID. Example: VLAN 1
USBdiag <*string*>	Specifies the filename of the diagnostic image to load from the USB. Example: vsp7000/vsp7000_10.0.1.10.bin

Parameter	Description
USBascii <*string*>	Specifies the filename of the ASCII config file to load from the USB. Example: customer1.cfg
USBagent <*string*>	Specifies the filename of the agent image to load from the USB and specifies IPs for next boot. Example: vsp7000/ vsp7000_10.0.1.0.img
NEXTIP, NEXTMask, and NEXTGateway	Specifies IP addresses, nework mask, and gateway to be used once the switch is booted.

Note:

If you download an ASCII file or diag/image with an `ip.cfg` file, the specific ASCII file or diag/ image must be present on the USB device.

The `ip.cfg` file loads information from the ASCII configuration file in order of precedence. For example, the stack IP becomes 181.30.30.113 no matter what IP address is in the `ip.txt` file if you have an `ip.cfg` file with the following commands:

```
USBascii ip.txt IP 181.30.30.113
Mask 255.255.255.0
Gateway 181.30.30.254
```

The stack IP will be the IP address defined in the `ip.txt` file if you have an `ip.cfg` file with the following commands:

```
IP 181.30.30.113
Mask 255.255.255.0
Gateway 181.30.30.254
USBascii ip.txt
```

Note:

The `ip.cfg` file runs only on a base or standalone unit. The file cannot be more than 4096 bytes or contain more than 200 lines.

The following figure shows an example of an `ip.cfg` file.

```
#Any lines starting with a # are comments
#IP <xx.xx.xx.xx> specifies the IP address for the switch

IP 172.16.1.23

#Mask <xx.xx.xx.xx> specifies the network mask Mask 255.255.255.0
#Gateway <xx.xx.xx.xx> specified the default gateway Gateway 172.16.1.1
#SNMPread <string> specified the SNMP read community string SNMPread public
#SNMPwrite <string> specified the SNMP write community string SNMPwrite private
#VLAN <number> specified the management VLAN-ID VLAN 1
#USBdiag <string> specifies the filename of the diagnostic image to load (noreset)

USBdiag ers5600/ers5600_5.1.0.4.bin

#USBagent <string> specifies the filename of the agent image to load (noreset)

USBagent ers5600/ers5600_5.2.0.0.img

#USBascii <string> specifies the filename of the ASCII config file to load

USBascii customer1.cfg

#NEXTIP <xx.xx.xx.xx> specifies the IP address for the switch NEXTIP 172.16.1.23
#NEXTMask <xx.xx.xx.xx> specifies the network mask NEXTMask  255.255.255.0
#NEXTGateway <xx.xx.xx.xx> specified the default gateway NEXTGateway 172.16.1.1
```

Figure 1: ip.cfg file example

If the `ip.cfg` file specifies an image or agent code, the switch loads the software, even if the same version is already installed on the switch. Ensuring that the appropriate software is always upgraded on the units is the correct operation of `ip.cfg`.

Use the factory default command to reset the switch to the factory default after you insert the USB memory device in the USB port. The USB memory device must contain the properly formatted `ip.cfg` file in the root directory.

Note:

The system does not display a message to indicate the IP.CFG file progress, you need to connect to the switch after 3 minutes of booting to verify the IP.CFG operation. You can typically confirm the successful download of IP.CFG by using the ACLI show ip command. If the USB IP.CFG file download succeeded, all parameters read from the file show are present in the switch and part of the runtime configuration.

Configuring a Domain Name Server

Use this procedure to set the default DNS domain name for the switch.

Note:

This default domain name is appended to all DNS queries or commands that do not already contain a DNS domain name.

Procedure

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

```
ip domain-name <DNS_domain name>
```

Variable definitions

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

Variable	Value
<DNS_domain_name>	Specify the default domain name to be used. The default form of this command is default ip domain-name. The no form of this command is no ip domain-name.

Resolving domain names to IP addresses

Use this procedure to set the domain name servers the switch uses to resolve a domain name to an IP address.

About this task

A switch can have up to three domain name servers specified for this purpose.

Note:

To enter all three server addresses you must enter the command three times, each with a different server address.

Procedure

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

```
ip name-server [<ipv6_address> | <ip_address_1>]
ip name-server [<ipv6_address> | <ip_address_2>]
ip name-server [<ipv6_address> | <ip_address_3>]
```

Variable definitions

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

Note:

The IPv6 parameter is valid only for switches that support IPv6.

Variable	Value
ipv6_address	The IPv6 address of the domain name server used by the switch.
ip_address_1	The IP address of the domain name server used by the switch.
ip_address_2	Optional. The IP address of a domain name server to add to the list of servers used by the switch.
ip_address_3	Optional. The IP address of a domain name server to add to the list of servers used by the switch.
no ip name-server [<ipv6_address> | <ip_address_1>] no ip name-server [<ipv6_address> | <ip_address_2>] no ip name-server [<ipv6_address> | <ip_address_3>]	The no form of this command removes domain name servers from the list of servers used by the switch to resolve domain names to an IP address.

Clearing the IP address

Use this procedure to clear the IPv4 address and subnet mask or IPv6 address for a switch or a stack.

Note:

When the IP address or subnet mask is changed, connectivity to Telnet can be lost. Any new Telnet connection can be disabled and is required to connect to the serial console port to configure a new IP address.

About this task

This command sets the IP address and subnet mask for a stack, switch, or unit to all zeros (0).

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command for IPv4 addresses:

   ```
   no ip address {stack | switch | unit <1-8>}
   ```

OR

for IPv6 addresses, enter the following command:

```
no ipv6 address {stack | switch | unit <1-8>}
```

Setting the in-band default IP gateway address

Use this procedure to set the default IP gateway address for a switch or a stack.

Note:

When the IP gateway is changed, connectivity to Telnet can be lost.

Important:

Only one management default gateway can operate for each unit or stack. The out-of-band management default gateway takes precedence over the in-band management default gateway. Once an out-of-band management default gateway is configured, the in-band management address is reachable only through a directly attached subnet for the management VLAN.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. To configure the IPv4 address of the default gateway, enter the following command at the command prompt:

   ```
   ip default-gateway <A.B.C.D>
   ```

Deleting the in-band default IP gateway address

Use this procedure to delete the default IP gateway address.

Note:

When the IP gateway is changed, connectivity to Telnet can be lost.

Procedure

1. Log on to the Global Configuration mode in ACLI.

2. At the command prompt, enter the following command:

   ```
   no ip default-gateway
   ```

   OR

   ```
   no ipv6 default-gateway
   ```

Chapter 6: Configuring Telnet using ACLI

Use the procedures in this section to enable Telnet and connect to other switches.

Setting Telnet access

Use this procedure to configure the Telnet connection. Then you can use Telnet to access the ACLI and manage the switch.

Note:

Multiple users can access ACLI system simultaneously, through the serial port, Telnet, and modems. If out-of-band is enabled on each unit of a stack, then you have a telnet server running on each unit. Therefore, you can have four connections to each out-of-ban IP, resulting in 4 (serial connections) plus 8*4 telnet connections, for 36 on a stack of eight units. This does not include any SSH connections. All users can configure simultaneously.

Before you begin

- The management port must have an assigned IP address.
- Remote access must be enabled.

Procedure

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

```
telnet-access [enable | disable] [login-timeout <0-10>]
[retry <1-100>] [inactive-timeout <0-60>] [logging {none |
access | failures | all}] [source-ip <1-50> <51-100>
<A.B.C.D> <WORD>] [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 connection. DEFAULT: enable
login-timeout <0-10>	Specify in minutes the time to wait for Telnet and Console login before the connection closes. Enter an integer between 0 and 10. DEFAULT: 1 minute
retry <1-100>	Specify the number of times the user can enter an incorrect password before closing the connection. Enter an integer between 1 and 100. DEFAULT: 3
inactive-timeout <0-60>	Specify in minutes the duration for an inactive session to be terminated. DEFAULT: 15 minutes
logging {none | access | failures | all}	Specify the events whose details you want to store in the event log: • none — Do not save access events in the log. • access — Save only successful access events in the log. • failure — Save failed access events in the log. • all — Save all access events in the log. DEFAULT: all
[source-ip <1-50><*A.B.C.D*>]	Specify the source IP address from which connections are allowed. Enter the IP address in dotted-decimal notation.
[source-ip <51–100><*WORD*>]	Specify the source IPv6 address/prefix form which connections are allowed.
mask <*A.B.C.D*>	Specify the subnet mask from which connections are allowed; enter IP mask in dotted-decimal notation.
no telnet-access [source-ip [<1-50>]]	Set the no form of this command, which disables the Telnet connection for an IPv4 address and mask pair.

Variable	Value
	When you do not use the optional parameter, the source-ip list is cleared, meaning the first index is set to 0.0.0.0/0.0.0.0, the second to fiftieth indexes are set to 255.255.255.255/255.255.255.255. When you specify a source-ip address, the specified pair is set to 255.255.255.255/255.255.255.255 for indexes between 1 and 50.
no telnet-access [source-ip [<51-100>]]	Set the no form of this command, which disables the Telnet connection for an IPv6 address and mask pair. When you do not use the optional parameter, the source-ip list is cleared, meaning the fiftyfirst index is set to ::/0, and the fiftysecond to hundredth indexes are set to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128. When you specify a source-ip address, the specified pair is set to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/ 128 for indexes between 51 and 100.
default telnet-access	Set the Telnet settings to the default values.

Using Telnet to communicate with another switch

Use this procedure to establish communications with another switch during the current ACLI session.

About this task

You can establish communication with only one external switch at a time using the Telnet command.

Procedure

1. Log on to the User EXEC mode in ACLI.
2. At the command prompt, enter the following command to specify the IP address, or the DNS host name of the unit with which to communicate:

   ```
   telnet <A.B.C.D> | <ipv6_addr> | <dns_host_name>
   ```

   Note:

   The IPv6 parameter is valid only for switches that support IPv6.

Note:

You can use the key combination `Ctrl+]` to force quit a session.

Using ping to test communication with another switch

Use this procedure to determine if communication with another switch can be established.

Procedure

1. Log on to the User EXEC mode in ACLI.
2. At the command prompt, enter the following command to specify the IP address or the DNS host name of the unit to test:

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

Note:

The IPv6 parameter is valid only for switches that support IPv6.

Variable definitions

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

Variable	Value
<A.B.C.D> | <WORD> | <dns_host_name>	Specify the IP address, IPv6 address, or the DNS host name of the unit to test.
vrf *<vrf_name>*	Specify the VRF name.
datasize <64– 4096>	Specify the size of the ICMP packet to be sent. The data size range is from 64 to 4096 bytes.
count <1–9999> | continuous	Set the number of ICMP packets to be sent. The continuous mode sets the ping running until the user interrupts it by entering Ctrl +C.

Variable	Value
timeout | -t | <1–120>	Set the timeout using either the timeout with the -t parameter followed by the number of seconds the switch must wait before timing out.
interval <1–60>	Specify the number of seconds between transmitted packets.
debug	Provide additional output information such as the ICMP sequence number and the trip time.
source <*A.B.C.D*>	Specify the source IP address of ping.

Chapter 7: Configuring the console and USB port using ACLI

Use the procedures in this section to control access to a switch or stack.

Disabling or enabling the console port

Use this procedure to disable or enable the console port.

About this task

You can configure the console port to deny or allow users access to the console port on the switch or stack.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to disable the console port on a switch or stack unit:

   ```
   no serial-console [unit <1-8>] [enable]
   ```
3. At the command prompt, enter the following command to enable the console port on a switch or stack unit:

   ```
   serial-console [unit <1-8>] [enable]
   ```

   OR

   ```
   default serial-console [unit <1-8>] [enable]
   ```

Displaying the serial console port

Use the following procedure to display the operational status of the serial console ports on all switches.

Procedure

1. Log on to the User EXEC mode in ACLI.

2. At the command prompt, enter the following command:
   ```
   show serial-console [unit <1-8>]
   ```

Note:

The unit parameter is valid only for units in a stack.

Disabling or enabling the USB port

Use this procedure to disable or enable the USB port.

About this task

You can configure the USB port to deny or allow users access to the USB ports on the switch or stack.

Procedure

1. Log on to the Global Configuration mode in ACLI
2. At the command prompt, enter the following command to disable the USB port on a switch or stack unit:
   ```
   no usb-host-port [unit <1-8>] [enable]
   ```
3. At the command prompt, enter either of the following commands to enable the USB port on a switch or stack unit:
   ```
   usb-host-port [unit <1-8>] [enable]
   ```
   OR
   ```
   default usb-host-port [unit <1-8>] [enable]
   ```

Variable definitions

The following table describes the parameters for the **`usb-host-port`** command.

Variable	Value
unit<*1–8*>	Specifies the unit number of a switch in a stack. Value range of 1 to 8. Do not use the unit variable for a stand alone switch.

Displaying the USB ports

Use this procedure to display the operational status of the USB ports on a switch or stack.

Procedure

1. Log on the User EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show usb-host-port [unit <1-8>]
   ```

Displaying USB files

Use the following command to display the files or directory structure of a USB device on a switch or stack unit.

Before you begin

The USB host port must be enabled.

A supported USB device must be inserted into a USB port on the switch.

About this task

You can display files or directories of a USB device.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show usb-files {ascii <WORD> | binary <WORD> | dir <WORD> | tree | unit
   <1-8>}
   ```

Variable definitions

The following table describes the parameters for the **`show usb-files`** command.

Variable	Value
ascii <*WORD*>	Specifies to display the ASCII contents of a file.

Variable	Value
binary <*WORD*>	Specifies to display the binary contents of a file.
dir <*WORD*>	Specifies to display files from a specific directory.
tree	Specifies to list the subdirectory tree recursively
unit <*1–8*>	Specifies to display files from a USB device in a specific stack unit. Unit value range of 1 to 8.

Chapter 8: Configuring the switch using ACLI

Use the procedures in this section to configure your switch for the first time, copy the configuration to a storage device, or retrieve a saved configuration. There are also procedures for displaying or modifying the current configuration on the switch or for restoring the factory default configuration.

Avaya Energy Saver configuration

You can use Avaya Energy Saver (AES) to configure the switch to utilize energy more efficiently.

Configuring global AES

Use the following procedure to enable or disable the energy saving feature for the switch.

About this task

Avaya recommends disabling AES on uplink copper ports since activating or deactivating AES on copper ports will trigger a link down followed rapidly by a link up event. The best solution is to use fiber ports for uplinks since link status will not change when AES is activated or deactivated

Important:

If a switch is reset while energy-saver is activated, the PoE power saving calculation may not accurately reflect the power saving, and in some cases may display zero savings. This is because the switch did not have sufficient time to record PoE usage between the reset of the switch and energy-saver being reactivated. When energy saver is next activated, the PoE power saving calculation will be correctly updated.

Important:

Some RIP routes might be cleared when AES is activated or deactivated on the uplink ports. Routes are automatically recovered when routes are relearned.

Using `ip rip advertise-when-down enable` option on the IP interface affected by the link change will help to keep the routes learned.

Important:

OSPF neighbors can disconnect when AES is activated or deactivated on uplink ports. Because of this link status change, some OSPF routes are cleared from the routing tables and automatically recovered when routes are relearned.

Using the **ip ospf advertise-when-down enable** command for the IP interface affected by the link change will help the routes remain learned.

Procedure

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

   ```
   [no] [default] energy-saver [enable] [efficiency-mode] [poe-power-saving]
   ```

Variable definitions

The following table describes the parameters for the **energy-saver** command.

Variable	Value
[default]	Configures AES efficiency mode, POE power saving, or global AES to default values (disabled).
efficiency-mode	Enables AES efficiency mode. **Important:** You must ensure that SNTP is enabled before you can enable AES efficiency mode. **Important:** You must disable AES globally before you can modify AES efficiency mode. **Important:** When enabled, AES efficiency mode overrides custom AES scheduling and PoE power saving mode. You will be prompted to confirm that you want to enable AES efficiency mode before proceeding.
enable	Enables AES globally

Variable	Value
[no]	Disables AES efficiency mode, PoE power saving, or AES globally.
poe-power-saving	Enables POE power saving. **Important:** You must disable AES globally before you can modify POE power saving.

Configuring port-based AES

Use this procedure to enable or disable energy saving for the accessed port, an alternate individual port, or a range of ports.

Before you begin

Disable AES globally.

Procedure

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

```
[no] [default] energy-saver [port <portlist>] [enable]
```

Variable definitions

The following table describes the parameters for the **`energy-saver port`** command.

Variable	Value
[default]	Configures energy savings to default values (disabled).
enable	Enables AES for the accessed port.
[no]	Disables AES for the accessed port, an alternate port, or list of ports.
port <portlist>	Specifies the port or list of ports for AES settings. **Important:** If you omit this parameter, the system uses the port number you specified when

Variable	Value
	you issued the interface command to enter the Interface Configuration mode.

Activating or deactivating AES manually

Use this procedure to have AES enabled, but not activated. Activate AES to ensure the AES is enabled and activated.

Before you begin

- Disable AES globally

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command to activate AES:
   ```
   energy-saver activate
   ```
3. At the command prompt, enter the following command to deactivate AES
   ```
   energy-saver deactivate
   ```

Configuring AES scheduling

Use this procedure to configure an on and off time interval for the switch to enter lower power states. The time interval can be a complete week, complete weekend, or individual days.

Before you begin

- Disable AES globally

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   energy-saver schedule {weekday|weekend|monday|tuesday|
   wednesday|thursday|friday|saturday|sunday} <hh:mm>
   {activate|deactivate}
   ```

Variable definitions

The following table describes the parameters for the **energy-saver schedule** command.

Variable	Value
activate	Specifies the AES on time.
deactivate	Specifies the AES off time.
friday|monday|saturday|sunday|thursday|tuesday|wednesday	Configures AES scheduling for a specific day.
<hh:mm>	Specifies the scheduled AES start time (hour and minutes).
weekday	Configures AES scheduling for all weekdays.
weekend	Configures AES scheduling for Saturday and Sunday.

Configuring AES scheduling to default

Use this procedure to completely disable scheduling for the switch or to disable specific energy saver schedules.

Before you begin

- Disable AES globally

Procedure

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

Variable definitions

The following table describes the parameters for the **default energy-saver schedule** command.

Variable	Value
friday|monday|saturday|sunday|thursday|tuesday|wednesday	Configures AES scheduling for a specific day to default (disabled).
<hh:mm>	Specifies the scheduled AES start time (hour and minutes).
weekday	Configures AES scheduling for all weekdays to default (disabled).
weekend	Configures AES scheduling for Saturday and Sunday to default (disabled).

Disabling AES scheduling

Use this procedure to discontinue using an on and off time interval for the switch to enter lower power states.

Before you begin

- Disable AES globally

Procedure

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

```
no energy-saver schedule
```

Variable definitions

The following table describes the parameters for the **no energy-saver schedule** command.

Variable	Value
friday|monday|saturday|sunday|thursday|tuesday|wednesday	Disables AES scheduling for a specific day.

Variable	Value
<hh:mm>	Specifies the scheduled AES start time (hour and minutes).
weekday	Disables AES scheduling for all weekdays.
weekend	Disables AES scheduling for Saturday and Sunday.

Viewing AES scheduling

Use this procedure to review configured energy saving schedule information.

Procedure

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

Viewing AES savings

Use this procedure to review the switch capacity energy saving (Watts) and the PoE energy savings (Watts).

Procedure

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

Viewing the global AES configuration

Use this procedure to review the AES configuration for the switch.

Procedure

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

```
show energy-saver
```

Viewing port-based AES configuration

Use this procedure to review AES configuration for all ports on the switch, an individual port, or range of ports.

Procedure

1. Log on to the User EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show energy-saver interface <portlist>
   ```

Variable definitions

The following table describes the parameters for the **`show energy-saver interface`** command.

Variable	Value
<portlist>	Specifies a port or range of ports.

Multiple switch configuration management

The Avaya Ethernet Routing Switch 5000 Series supports the storage of two switch configurations in flash memory. The switch can use either configuration and must be reset in order for the configuration change to take effect.

A regular reset of the switch synchronizes any configuration changes to the active configuration whereas a reset to defaults causes the active configuration to be set to factory defaults. The inactive block is not affected.

In stack configurations, all units in the stack must use the same active configuration. If a unit joins a stack, a check is performed between the unit's active configuration and the stack's active configuration. If the two are not the same, the new stack unit resets and loads the stack's active configuration.

Displaying the stored configurations

Use this procedure to show the configurations currently stored on the switch.

Procedure

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

Displaying the current configuration

Use this procedure to display the current configuration of a switch or a stack for switches that support stacking.

Procedure

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

Note:

If the switch CPU is busy performing other tasks, the output of this command can appear to intermittently start and stop. This is a normal operation to ensure that the switch management tasks receive appropriate priority.

Variable definitions

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

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

Variable	Value
	[802.1AB] [aaur][adac] [arp-inspection] [asset-id][aur][banner] [brouter][core] [default-cmd-interface][dhcp-relay] [dhcp-snooping] [eap] [energy-saver][igmp] [interface] [ip] [ip-source-guard] [ipfix][ipmgr] [ipv6] [l3] [l3-protocols] [lacp] [logging] [mac-security] [mld][mlt][pim][poe] [port-mirroring] [qos] [rate-limit] [rmon] [rtc][slamon] [slpp] [smlt][snmp] [ssh] [sshc][ssl] [stack][stkmon] [stp] [unicast-storm-control][vlacp] [vlan] **Note:** Not all switches support the variables listed for the module <value> parameter.

Restoring the factory default configuration

Use this procedure to reset the switch or stack back to its default configuration.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   `restore factory-default [-y]`
   The [-y] parameter instructs the switch not to prompt for confirmation.

Configuring with IP Office Script

Use this procedure to automatically configure parameters for the ERS 5600 switch.

Before you begin

Avaya recommends you to execute the ACLI command **`run ipoffice`** on an ERS 5600 switch operating in a factory default state.

About this task

The run ipoffice command executes a script containing many switch configuration parameters to optimize the ERS 5600 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.

Procedure

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

Example

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

```
5650TD-PWR>en
5650TD-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 set 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.
% ------------------------------------------------------------------------
5650TD-PWR+#
```

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

```
5650TD-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] :
Voice VLAN Gateway IP Address [192.168.42.254] :10.10.42.254
Voice VLAN Gateway IP Mask [255.255.255.0] :
Data VLANI ID [44] :
Data VLAN Gateway IP Address [192.168.44.254] :10.10.44.254
Data VLAN Gateway IP Mask [255.255.255.0] :
IP Route to Gateway Modem-Router (Internet/WAN) [192.168.44.2] :10.10.44.99
IP Office Call-Server IP address [192.168.42.1] :10.10.42.200
IP Office File-Server IP address [192.168.42.1] :10.10.42.200
% The Voice VLAN ID has been set to 42
% 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
% 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
% ------------------------------------------------------------------
% Default IP Route set to 10.10.44.99 (Gateway Modem-Router interface)
% IP Office Call-Server IP address is set to 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.
% ------------------------------------------------------------------
5650TD-PWR+#
```

Configuring with ADAC script

Use the following procedure to configure parameters for ADAC using the run ADAC script.

Before you begin

Avaya recommends you execute the ACLI command **`run adac`** on an ERS 5600 switch operating in a factory default state.

About this task

Note:

You cannot set VLAN 1 (default VLAN) as the voice VLAN ID.

Procedure

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

Example

The following is a sample output of the **run adac** command script

```
5650TD# run adac
*********************************************************
*** This script will guide you through configuring the ***
*** Avaya switch for optimal operation using ADAC.     ***
*** ---------------------------------------------------***
*** Input required values at each prompts.             ***
*** If you wish to terminate or exit this script       ***
*** enter ^C <control-C> at any prompt.                ***
*** Warning: This script may delete previous settings. ***
*********************************************************
Data VLAN ID [2-4094 or Enter to skip]: 4093
Do you want to use the Data VLAN as the management VLAN [Y/N]? y
```

```
Default IP Route [A.B.C.D]: 10.100.100.254
Management IP address [A.B.C.D or Enter to skip]: 10.100.100.1
Management IP netmask [xxx.xxx.xxx.xxx or Enter to skip]: 255.255.255.0
Voice VLAN ID [2-4094]: 1000
Voice VLAN Gateway IP address [A.B.C.D or Enter to skip]: 10.50.50.1
Voice VLAN Gateway IP netmask [xxx.xxx.xxx.xxx/xx]: 255.255.255.0
LLDP Call-Server IP address [A.B.C.D]: 10.40.40.1
LLDP File-Server IP address [A.B.C.D]: 10.30.30.1
Do you want to configure a MLT Trunk as Uplink port? [Y/N] n
ADAC Uplink ports [slot/port,slot/port...]: 1/10,1/11
ADAC Call Server ports [slot/port,slot/port...]: 1/20,1/21
ADAC Telephony ports [slot/port,slot/port...]: 1/25,1/26
% The Data VLAN ID is set to 4093
% Management VLAN is now set to 4093
% The Default IP Route is set to 10.100.100.254
% The Management IP address is set to 10.100.100.1
% The Management IP netmask is set to 255.255.255.0
% The Voice VLAN ID is set to 1000
% The Voice VLAN Gateway IP address is set to 10.50.50.1
% The Voice VLAN Gateway IP netmask is set to 255.255.255.0
% LLDP Call Server IP address is set to 10.40.40.1
% LLDP File Server IP address is set to 10.30.30.1
% ADAC Uplink ports are set to 1/10,1/11
% ADAC is now enabled
% ADAC Call Server ports set to 1/20,1/21
% ADAC Telephony ports set to 1/25,1/26
% ** Switch QoS and Unified Communications policies setup and saved **
% ------------------------------------------------------------------------
% To manage this Avaya switch, enter 10.100.100.1 in your Web browser.
% ------------------------------------------------------------------------
5650TD#
```

Configuring with LLDP Script

Use this procedure to configure or modify LLDP and Voice VLAN using VLAN ID, IP addresses, LLDP MED policies, and QoS rules.

Before you begin

Avaya recommends you execute the ACLI command **`run lldp`** on an ERS 5600 switch operating in a factory default state.

About this task

Procedure

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

   ```
   run lldp
   ```

3. Enter the information requested at each prompt.

Example

The following is a sample output of the **run lldp** command script

```
5650TD#run lldp
*********************************************************
*** This script will guide you through configuring the ***
*** Avaya switch for optimal operation using LLDP.     ***
*** ---------------------------------------------------***
*** Input required values at each prompts.             ***
*** If you wish to terminate or exit this script       ***
*** enter ^C <control-C> at any prompt.                ***
*** Warning: This script may delete previous settings. ***
*********************************************************
Data VLAN ID [2-4094 or Enter to skip]: 4093
Do you want to use the Data VLAN as the management VLAN [Y/N]? y
Default IP Route [A.B.C.D]: 10.100.100.254
Data VLAN Uplink ports [slot/port,slot/port... ]: 1/10,1/11
Management IP address [A.B.C.D or Enter to skip]: 10.100.100.1
Management IP netmask [xxx.xxx.xxx.xxx/xx]: 255.255.255.0
Voice VLAN ID [2-4094]: 1000
Voice VLAN Gateway IP address [A.B.C.D or Enter to skip]: 10.50.50.1
Voice VLAN Gateway IP netmask [xxx.xxx.xxx.xxx/xx]: 255.255.255.0
LLDP Call-Server IP address [A.B.C.D]: 10.40.40.1
LLDP File-Server IP address [A.B.C.D]: 10.30.30.1
% The Data VLAN ID is set to 4093
% Management VLAN is now set to 4093
% The Default IP Route is set to 10.100.100.254
% The Data VLAN Uplink ports 1/10,1/11 tagging is set to tagAll
% The Management IP address is set to 10.100.100.1
% The Management IP netmask is set to 255.255.255.0
% The Voice VLAN ID is set to 1000
% The Voice VLAN Gateway IP address is set to 10.50.50.1
% The Voice VLAN Gateway IP netmask is set to 255.255.255.0
% LLDP Call Server IP address is set to 10.40.40.1
% LLDP File Server IP address is set to 10.30.30.1
% ** Switch QoS and Unified Communications policies setup **
% ------------------------------------------------------------------------
% To manage this Avaya switch, enter 10.100.100.1 in your Web browser.
% ------------------------------------------------------------------------


5650TD#
```

Copying a configuration to flash memory

Use this procedure to copy the current configuration to one of the flash memory spots.

Procedure

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

```
copy config nvram [block <1-2> name <block_name>]
```

Variable definitions

The following table describes the parameters for the **copy config nvram block** command.

Variable	Value
<1–2>	The flash memory location to store the configuration.
name <block_name>	The name to attach to this block. Names can be up to 40 characters in length with no spaces.

Copying a configuration from flash memory

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   copy nvram config block <1-2>
   ```
   Substitute <1-2> with the configuration file to load. This command causes the switch to reset so that the new configuration can be loaded.

Copying the running configuration to a USB device

Use this procedure to copy the running configuration file to a USB mass storage device.

Procedure

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

```
copy running-config usb {[module <value>] | [verbose]}
filename <WORD>
```

Variable definitions

The following table describes the parameters for the **copy running-config usb** command.

Variable	Value
module <value>	Copies the configuration of an application for any of the following parameter values that the switch supports: [banner] [core] [interface] [ip] [ipmgr] [logging] [macsecurity] [mlt] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [stack] [stp] [vlan] **Note:** Not all switches support the variables listed for the module <value> parameter.
verbose	Copies all the configuration, including defaults and non-defaults, to the USB.
filename <WORD>	Specifies the name of the file that is created when the configuration is saved to the USB mass storage device.

Restoring a system configuration from a USB device

Use this procedure to restore a configuration file stored on a USB mass storage device.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   copy usb config filename <name>
   ```

   Note:

   The only parameter for this command is the name of the file to be retrieved from the USB device.

Configuring a TFTP server IP address

Use the following commands to configure a default TFTP server IP address on the switch.

About this task

To save time and prevent input errors, you can store a default TFTP server IP address on the switch so that the system can use that address automatically for the *tftp* parameter in TFTP server related procedures. For example:

- Changing switch software using ACLI
- Copying the running configuration to a TFTP server
- Restoring the system configuration from a TFTP server

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command To specify a default TFTP server IP address:

   ```
   tftp-server {<A.B.C.D> | <WORD>}
   ```

3. At the command prompt, enter one of the following commands To clear the default TFTP server IP address:

   ```
   no tftp-server
   ```

   OR

   ```
   default tftp-server
   ```

Next steps

To display the current TFTP server IP address, enter the following command:

```
show tftp-server
```

Variable definitions

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

Variable	Value
<*A.B.C.D*>	Specifies an IPv4 address for the TFTP server.
<*WORD*>	Specifies an IPv6 address for the TFTP server.

Configuring an SFTP server IP address

Use the following commands to configure a default SFTP server IP address on the switch.

Before you begin

The switch must be running a secure software image to support SFTP.

About this task

To save time and prevent input errors, you can store a default SFTP server IP address on the switch so that the system can use that address automatically for the *sftp* parameter in SFTP server related procedures. For example:

- Changing switch software using ACLI
- Copying the running configuration to a SFTP server
- Restoring the system configuration from a SFTP server

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to specify a default SFTP server IP address:

   ```
   sftp-server {<A.B.C.D> | <WORD>}
   ```

3. At the command prompt, enter the following command to clear the default SFTP server IP address:

   ```
   no sftp-server
   ```

   OR

   ```
   default sftp-server
   ```

Next steps

To display the current SFTP server IP address, enter the following command:

```
show sftp-server
```

Variable definitions

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

Variable	Value
<*A.B.C.D*>	Specifies an IPv4 address for the SFTP server.
<*WORD*>	Specifies an IPv6 address for the SFTP server.

Copying the running configuration to a TFTP or SFTP server

Use this procedure to copy the running configuration file to a TFTP or SFTP server.

Before you begin

The switch must be running a secure software image to support SFTP.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. Log on to the Privileged EXEC mode in ACLI.
3. At the command prompt, enter the following command to copy the running configuration to a TFTP server:
   ```
   copy running-config tftp address {<A.B.C.D> | <WORD>}
   {[module <value>] | [verbose]} filename <WORD>
   ```
4. At the command prompt, enter the following command to copy the running configuration to a SFTP server:
   ```
   copy running-config sftp address {<A.B.C.D> | <WORD>}
   {[module <value>] | [verbose]} filename <WORD> username
   <WORD>
   ```

Variable definitions

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

Variable	Value
address {<A.B.C.D> | <WORD>}	Specifies the address of the server to be used: • *A.B.C.D* specifies the IP address. • *WORD* specifies the IPv6 address.
verbose	Copies all the configuration parameters including defaults and non-defaults.
module <value>	Copies the configuration of an application for any of the following parameter values that the switch supports: [banner] [core] [interface] [ip] [ipmgr] [logging] [mlt] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [stp] [vlan] **Note:** Not all switches support the variables listed for the module <value> parameter.
filename <WORD>	Specifies the name of the file that is created when the configuration is saved to the server.
username <WORD>	Specifies the username to access the SFTP server. **Note:** If password authentication is configured, a password is required.

Restoring a configuration from a binary file from a TFTP or SFTP server

Use this procedure to restore a configuration from a binary file stored on a TFTP or SFTP server.

Before you begin

The switch must be running a secure software image to support SFTP.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. At the command prompt, enter the following command to restore a configuration file from a TFTP server:
   ```
   copy tftp config address {<A.B.C.D> | <WORD>} filename <name>
   ```
3. At the command prompt, enter the following command to restore a configuration file from a SFTP server:
   ```
   copy sftp config address {<A.B.C.D> | <WORD>} filename <name>
   username <WORD>
   ```

Variable definitions

The following table describes the parameters for the **`copy tftp config`** and **`copy sftp config`** commands.

Variable	Value
address {<A.B.C.D> | <WORD>}	Specifies the address of the server to be used: • *A.B.C.D* specifies the IP address. • *WORD* specifies the IPv6 address.
filename <name>	The name of the file to be retrieved.
username <WORD>	Specifies a username to access the SFTP server. **Note:** If password authentication is configured, a password is required.

Storing configuration in binary files on a TFTP or SFTP server

Before you begin

The switch must be running a secure software image to support SFTP.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. At the command prompt, enter the following command to store configuration in a binary file on a TFTP server:
   ```
   copy config tftp address {<A.B.C.D> | <WORD>} filename <name>
   ```
3. At the command prompt, enter the following command to store configuration in a binary file on an SFTP server:
   ```
   copy config sftp address {<A.B.C.D> | <WORD>} filename <name>
   ```

Example

Variable definitions

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

Variable	Value
address*[<A.B.C.D> | <WORD>}*	Specifies the address of the server to be used: • A.B.C.D specifies the IP address • WORD specifies the IPv6 address
filename<*WORD*>	Specifies the name of the file that that is created when the configuration is saved ot the server.

Loading a configuration file automatically at startup from USB

Use the following command to configure loading and executing a file from a USB device during boot.

About this task

You can enable a switch or stack to load and execute a script file from a USB device during boot.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   configure usb load-on-boot {disable | use-config} filename <name>
   ```

Next steps

To view the USB load on boot settings, enter the following command:

```
show config-usb-loadonboot
```

Variable definitions

The following table describes the parameters for the **`configure usb load-on-boot`** command.

Variable	Value
{disable| use-config}	Specifies the settings for automatically loading a configuration file from USB when the system boots: • `disable` disables the automatic loading of the ASCII configuration file. • `use-config` specifies loading the ASCII configuration file at boot from a USB device. **Note:** If you omit this parameter, the system immediately downloads and runs the ASCII configuration file.
filename <name>	Specifies the name of the configuration file to use in this process.

Configuring an automatic file download at startup

Use the following command to configure loading and executing a file from the network during boot.

About this task

You can enable a switch or stack to load and execute a script file and configure parameters to automatically download a configuration file from the network during boot.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. At the command prompt, enter the following command:
   ```
   configure network load-on-boot {disable | use-bootp | use-config} address {<A.B.C.D> | <ipv6addr>} filename <name>
   ```

Next steps

To view the network load on boot settings, enter the following command:

```
show config-network
```

Variable definitions

The following table describes the parameters for the **`configure network load-on-boot`** command.

Variable	Value
{disable | usebootp | useconfig}	Specifies the settings for automatically loading a configuration file when the system boots: • disable disables the automatic loading of the config file. • use-bootp specifies loading the ASCII configuration file at boot and using BootP to obtain values for the TFTP address and filename. • use-config specifies loading the ASCII configuration file at boot and using the

Variable	Value
	locally configured values for the TFTP address and filename. **Note:** If you omit this parameter, the system immediately downloads and runs the ASCII config file.
address <A.B.C.D>	Specifies the IP address of the desired TFTP server.
filename <name>	Specifies the name of the configuration file to use in this process.

Configuring Autosave

Use the following commands to enable or disable the Autosave feature.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to enable Autosave:
   ```
   autosave enable
   ```
   With Autosave enabled, the system checks for new configuration data every minute, and automatically saves new data to NVRAM. While Autosave is enabled, the AUR feature performs normally.
3. At the command prompt, enter the following command to disable Autosave:
   ```
   no autosave enable
   ```
   With Autosave disabled, the unit will not save the new configuration data to NVRAM. The user can use AUR to restore all the configuration data that is configured before the feature is disabled. With AUR, You can also restore all the configuration data that is configured before the ACLI command **`copy config nvram`** is executed. When resetting a stack with Autosave disabled, the stack will form with the configuration from NVRAM of each unit in the stack. The original configuration of a unit is restored if the user replaces that unit in the stack without having to use the **`copy config nvram`** command.

Displaying hardware information

Use this procedure to display hardware information about the status of the switch.

Procedure

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

Note:

With the verbose option, you can display additional information such as fan status, power status, and the switch serial number.

Configuring the Asset ID

Use the following commands to configure the Asset ID for the switch, stack, or unit.

About this task

You can configure an Asset ID to provide inventory information for the switch, stack, or each unit in a stack. An Asset ID consists of an alphanumeric string of up to 32 characters in length. An Asset ID is useful for recording your company specific asset tracking information, such as an asset tag attached to the unit.

Procedure

1. Logon to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to configure the Asset ID string:
   ```
   asset-id [stack|unit <1-8>] <WORD>
   ```
3. To disable the Asset ID string, enter the following command:
   ```
   no asset-id [stack|unit <1-8>]
   ```
4. To default the Asset ID string, enter the following command:

```
default asset-id [stack|unit <1-8>]
```

Example

The following example configures an Asset ID of AVA1234 for unit 3 in the stack:

```
asset-id unit 3 AVA1234
```

Note:

To configure the Asset ID of a standalone switch, do not enter a stack or unit parameter.

Next steps

To verify the Asset ID string settings for both a switch and stack, use the **`show sys-info`** command. For more information, see Displaying system information on page 118.

To verify the Asset ID string settings for a stack only, use the **`show system`** command. For more information, see Displaying consolidated system information on page 119.

To verify the Asset ID string settings for a switch only, use the **`show system verbose`** command. For more information, see Displaying verbose system information on page 119.

Variable definitions

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

Variable	Value
stack	Configure the Asset ID of the stack.
unit <1–8>	Configure the Asset ID of a unit in the stack. Unit value of 1 to 8.
<WORD>	Enter the Asset ID. Alphanumeric up to 32 characters. You can specify the Asset ID within double quotation marks (i.e. ” ”) to include embedded spaces.

Configuring SNMP

Use this procedure to configure Simple Network Management Protocol (SNMP) to monitor devices running software that supports the retrieval of SNMP information.

Procedure

1. Log on to the Global Configuration mode in ACLI.

2. At the command prompt, enter the following command to enable SNMP. (The default setting is disabled.)
   ```
   snmp-server enable
   ```
3. Enable authentication traps.
   ```
   snmp-server authenticationtrap enable
   ```
4. Set the read-only community name (requirement: enter community string twice).
   ```
   snmp-server community ro
   ```
5. Set the read-write community name (requirement: enter community string twice).
   ```
   snmp-server community rw
   ```
6. Set contact information.
   ```
   snmp-server contact "whatever you want"
   ```
7. Set building name and closet information.
   ```
   snmp-server location <Building/Closet-number>
   ```
8. Maintain coherent Syslog messages.
   ```
   snmp-server name <switch_ipaddress>
   ```
9. Set IP address of trap receiver.
   ```
   snmp-server host <host IP> <community-string>
   ```
10. Verify configuration.
    ```
    show sys-info
    ```
11. Verify configuration.
    ```
    show snmp host
    ```

Configuring VLANs and tagged uplinks

Use the following procedure to configure Virtual Local Area Networks (VLAN) and tagged uplinks.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to automatically remove an untagged port from current VLAN and update PVID when the port is added to a different VLAN. (The setting appears at the bottom of the VLAN configuration information.)
   ```
   vlan configcontrol automatic
   ```
3. Enable tagging on the uplink.

```
vlan ports <uplink port> tagging tagall
```

4. Discard untagged frames.
   ```
   vlan ports <uplink port> filter-untagged-frame enable
   ```
5. Break Spanning Tree Protocol (STP) for Voice over Internet Protocol (VoIP).
   ```
   vlan ports ALL filter-unregistered-frame disable
   ```
6. Create the port based VLAN and assign the 802.1q identifier.
   ```
   vlan create <vid> type port
   ```
7. Name the VLAN according to conventions.
   ```
   vlan name <vid> <name>
   ```
8. Add ports to appropriate VLANs.
   ```
   vlan members add <vid> <port_listing>
   ```
9. Set the management VLAN.
   ```
   vlan mgmt <vid>
   ```
10. Remove all ports from VLAN 1.
    ```
    vlan members remove 1 ALL
    ```
11. Set the PVID on the uplink.
    ```
    vlan ports <uplink_port> pvid <vid>
    ```
12. Verify VLAN configuration.
    ```
    show vlan
    ```
13. Verify configuration of PVID and port type.
    ```
    show vlan interface info
    ```

Configuring IGMP

Use this procedure to configure Internet Group Management Protocol (IGMP) to manage multicast group members that IP multicast routers use to learn the existence of multicast group members on their directly attached subnets.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to enable IGMP snooping on each appropriate VLAN.
   ```
   vlan igmp <vid> snooping enable
   ```
3. Enable IGMP proxy on each appropriate VLAN.

```
vlan igmp <vid> proxy enable
```

4. Show IGMP information for each appropriate VLAN.

```
show vlan igmp <vid>
```

System clock configuration

The following sections provide information you can use to configure the switch system clock.

You can perform clock tasks such as setting the clock source, setting the local time zone, configuring Simple Network Time Protocol (SNTP), configuring SNTP synchronization, or configuring daylight savings time.

Setting the real-time clock

Use this procedure to set the real-time clock (RTC), providing the switch with time information. The RTC provides the switch with time information in the instance that SNTP time is not available.

Procedure

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

```
clock set {<LINE> | <hh:mm:ss>}
```

Variable definitions

The following table describes the parameters for the **`clock set`** command.

Variable	Value
<LINE>	Specify a string in the format of mmddyyyyhhmmss that defines the current local time.
<hh:mm:ss>	Specify the current local time in the hh:mm:ss format.

Setting the default clock source

Use this procedure to set the default clock source for the switch.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   clock source {sntp | rtc | sysUpTime}
   ```

Variable definitions

The following table describes the parameters for the **`clock source`** command.

Variable	Value
sntp	Specifies Simple Network Time Protocol (SNTP) as the time source.
rtc	Specifies Real Time Clock (RTC) as the time source.
sysUpTime	Specifies System Up Time as the time source.

Resetting the clock source to factory default

Use this procedure to restore the clock source to factory defaults.

Procedure

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

Enabling or disabling SNTP

Use the following procedure to enable or disable Simple Network Time Protocol (SNTP).

About this task

The Simple Network Time Protocol (SNTP) feature synchronizes the Universal Coordinated Time (UCT) 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.

Using SNTP provides a real-time timestamp for the software, shown as Greenwich Mean Time (GMT). If SNTP is enabled, the system synchronizes with the configured NTP server at boot-up and at user-configurable periods thereafter (the default synchronization interval is 24 hours). The first synchronization is not performed until network connectivity is established. SNTP supports primary and secondary NTP servers. The system tries the secondary NTP server only if the primary NTP server is unresponsive.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to enable SNTP:
   ```
   sntp enable
   ```
3. At the command prompt, enter the following command to disable SNTP:
   ```
   no sntp enable
   ```

Important:

The default setting for SNTP is *disabled*.

Configuring the SNTP server

Use this procedure to configure the primary and secondary SNTP server IP addresses.

About this task

You can configure the Network Time Protocol (NTP) servers for SNTP.

Important:

If problems occur when you use SNTP, try various NTP servers. Some NTP servers can be overloaded or currently inoperable. The system retries connecting with the NTP server a maximum of three times, with 5 minutes between each retry.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to configure the SNTP primary address:
   ```
   sntp server primary address [<ipv6address> | <A.B.C.D>]
   ```
3. At the command prompt, enter the following command to configure the SNTP secondary address:
   ```
   sntp server secondary address [<ipv6address> | <A.B.C.D>]
   ```
4. At the command prompt, enter the following command to clear an SNTP address:
   ```
   no sntp server {primary | secondary}
   ```

Variable definitions

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

Variable	Value
<ipv6address>	Enter the IPv6 address of the SNTP server.
<A.B.C.D>	Enter the IP address of the SNTP server.
primary	Specifies the primary SNTP server.
secondary	Specifies the secondary SNTP server.

Setting SNTP snychronization

Use the following commands to perform a manual synchronization or to configure a recurring synchronization.

Before you begin

SNTP must be enabled.

About this task

You can perform and manual synchronization with the SNTP server, or configure a recurring synchronization with the secondary SNTP server in hours relative to the initial synchronization.

Procedure

1. Log on to the Global Configuration mode in ACLI.

2. At the command prompt, enter the following command to force a manual synchronization:
   ```
   sntp sync-now
   ```
3. At the command prompt, enter the following command to configure a recurring synchronization:
   ```
   sntp sync-interval <0-168>
   ```

   Important:

   Enter the number of hours between a recurring SNTP server synchronization. 0 is boot time only, 168 is once a week.

Synchronizing the clock with SNTP

Use the following procedure to enable the RTC to synchronize with the SNTP clock.

Before you begin

SNTP must be enabled.

About this task

You can configure the RTC to synchronize with the SNTP clock when the SNTP clock synchronizes.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   clock sync-rtc-with-ntp enable
   ```

Disabling clock and SNTP synchronization

Use this procedure to disable the synching of the RTC with the SNTP clock when the SNTP clock synchronizes.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   no clock sync-rtc-with-ntp enable
   ```

Resetting clock synchronization to default

Use this procedure to restore the synchronizing of the RTC with the SNTP clock to factory defaults.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   default clock sync-rtc-with-ntp enable
   ```

Setting the local time zone

Use the following procedure to configure the clock time zone.

Before you begin

SNTP must be enabled.

About this task

You can configure your switch clock for your local time zone.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   clock time-zone <zone> <hours> [minutes]
   ```

Example

The following command sets the time zone to UTP minus 8 hours and the time zone displays as PST.

```
clock time-zone PST -8
```

Variable definitions

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

Variable	Value
<zone>	Specifies the time zone acronym to display when showing system time (up to 4 characters), for example EST for Eastern Standard Time, or PST for Pacific Standard Time.
<hours>	Enter the difference from UTC in hours. Value range between –12 and +12.
[minutes]	Optional: Enter the difference from UTC in minutes. Value range between 0 and 59.

Setting daylight savings time

Use the following procedure to set the daylight savings time change dates.

About this task

You can configure the clock change dates for daylight savings time.

Procedure

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

```
clock summer-time <zone> [date <day> <month> <year> <hh:mm>
<end-day> <end-month> <end-year> <end-hh:mm>] [offset]
```

Example

The following command sets the daylight savings time to begin on March 13 2011 at 2AM and end on November 6 2011 at 2AM.

```
clock summer-time PST date 13 March 2011 2:00 6 November 2011 2:00 +60
```

Variable definitions

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

Variable	Value
<*zone*>	Specifies the time zone acronym to display when daylight savings time is in effect. If unspecified, the default is the current time zone acronym.
date	Specifies daylight savings time to start and end on the following dates.
<*day*>	Specifies the start day.
<*month*>	Specifies the start month.
<*year*>	Specifies the start year.
<*hh:mm*>	Specifies the hour and minute to start daylight savings time.
<*end-day*>	Specifies the end day.
<*end-month*>	Specifies the end month.
<*end-year*>	Specifies the end year.
<*end-hh:mmy*>	Specifies the hour and minute to end daylight savings time.
[offset]	Specifies the number of minutes to add for daylight savings time. (-840 to 840)

Setting recurring daylight savings time

Use this procedure to configure recurring daylight savings time start and end dates.

About this task

You can configure the clock daylight savings time to recur annually.

Procedure

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

```
clock summer-time recurring {<startWeek:1-5|last>}
<start:DAY> <start:MONTH> <start:dd:mm> {<endWeek:1-5>|
last>} <end:DAY> <end:MONTH> <end:hh:mm> [offset <1-1440>]
```

Example

The following command configures the recurring daylight savings time to start on day 13 of the third week in March, and end on day 6of the second week in November.

```
clock summer-time recurring 3 13 March 02:00 2 6 November 02:00 offset
60
```

Variable definitions

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

Variable	Value
<startWeek:1–5> | last>	Specifies the week of the month (starting on Sunday) you want recurring daylight savings time to start. Values include: • <1–5> — the first to the fifth week for months of the year that include five Sundays. • last — the last week of months of the year that do not include five Sundays. **Note:** For the <1–5> parameter, weeks count from the first day of the month, not calendar weeks. Therefore, weeks 1–4 may not always apply. Week 5 may not apply in certain years. In that case, summer time start/end uses the last parameter. For years without a Sunday in the fifth week of March, summer time starts on the last Sunday of March.
<start:DAY>	Specifies the day recurring daylight savings time starts.
<start:MONTH>	Specifies the month recurring daylight savings time starts.
<start:hh:mm>	Specifies the hour and minutes of the day recurring daylight savings time starts.

Variable	Value
<*endWeek:1–5*> | *last*>	Specifies the week of the month (starting on Sunday) you want recurring daylight savings time to end. Values include: • <1–5> — the first to the fifth week for months of the year that include five Sundays. • last — the last week of months of the year that do not include five Sundays. **Note:** For the <1–5> parameter, weeks count from the first day of the month, not calendar weeks. Therefore, weeks 1–4 may not always apply. Week 5 may not apply in certain years. In that case, summer time start/end uses the last parameter.
<*end:DAY*>	Specifies the day recurring daylight savings time ends
<*end:MONTH*>	Specifies the month recurring daylight savings time ends.
<*end:hh:mm*>	Specifies the hour and minutes of the day recurring daylight savings time ends.
offset<*1–1440*>	Specifies the time change in minutes when daylight savings time starts and ends. The offset is added when daylight savings time begins, and subtracted when daylight savings time ends. Value range is 1 to 1440 minutes.

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. Enter Global Configuration mode:
   ```
   enable
   ```

```
configure terminal
```

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
   ```

Example

```
5650TD-PWR<config>#show clock
   System Clock time  :     FRI JAN 09 05:45:34 1970

    Current SNTP time  :     Not Set
    Daylight saving recurring time is disabled
    Daylight saving time is disabled
    Time zone offset from UTC is 00:00
5650TD-PWR<config>#cli timestamp enable
5650TD-PWR<config>#show clock
1970-01-09 05:45:48 GMT+00:00

   System Clock time  :     FRI JAN 09 05:45:49 1970

    Current SNTP time  :     Not Set
    Daylight saving recurring time is disabled
    Daylight saving time is disabled
    Time zone offset from UTC is 00:00
```

Configuring boot parameters

Use this procedure to perform a soft-boot of the switch or stack.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   boot [default] [partial—default] [primary] [secondary] [unit
   <1–8>]
   ```

Note:

When you reset to factory defaults, the switch or stack retains the last reset count and reason for last reset; these two parameters do not default to factory defaults. Stack operational mode is retained only when resetting to partial-default.

Variable definitions

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

Variable	Value
default	Reboot the stack or switch and use the factory default configurations.
partial-default	Reboot the stack or switch and use partial factory default configurations. This parameter retains the Management IP address, licenses, and passwords for console and telnet/Web. **Note:** You can use the partial-default parameter on a standalone switch or on an entire stack. You cannot boot individual units in a stack to partial-default.
primary	Reboot the stack or switch and use the primary agent image.
secondary	Reboot the stack or switch and use the secondary agent image.
unit <1–8>	Specify the unit number to reboot.

Configuring DHCP modes

Use this procedure to configure DHCP modes and automatically obtain an IP address, subnet mask and default gateway on the switch or stack. When you use DHCP, the switch or stack can also obtain up to three DNS server IP addresses.

Procedure

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

   ```
   ip address source {configured-address | dhcp-always | dhcp-lastaddress | dhcp-when-needed}
   ```

Variable definitions

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

Variable	Value
configured-address	Use the manually configured IP configuration.
dhcp-always	Always use the DHCP server.
dhcp-lastaddress	Use the last DHCP server.
dhcp-when-needed	Use DHCP client when needed.

Configuring BootP parameters

Use this procedure to configure BootP on the current instance of the switch or server.

Procedure

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. Log on to the Global Configuration mode in ACLI.
3. At the command prompt, enter the following command:
   ```
   ip bootp server {always | default-ip | disable | last}
   ```
4. To disable the BootP/DHCP server, enter the following command:
   ```
   no ip bootp server
   ```
5. To restore the default BootP server setting, enter the following command:
   ```
   default ip bootp server
   ```

Variable definitions

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

Variable	Value
always	Specifies to use BootP always.
default-ip	Specifies to use BootP or the default IP. This is the default value.
disable	Specifies to use BootP never.
last	Specifies to use BootP or the last known address.
default	Restores the default BootP server setting.
no	Disables the BootP/DHCP server

Displaying BootP and DHCP modes

Use this procedure to display the IP configurations, BootP/DHCP mode, stack address, switch address, subnet mask, and gateway address.

Procedure

1. Log on to the User EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show ip [bootp] [dhcp] [default-gateway] [address [source]]
   ```

Variable definitions

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

Variable	Value
bootp	Displays BootP/DHCP-related IP information. The possibilities for status returned are: • BootP Always • BootP or Last Address

Variable	Value
	• BootP When Needed • Disabled • DHCP Always • DHCP or Last Address • DHCP When Needed
dhcp client lease	Displays DHCP client lease information. The command displays information about configured lease time and lease time granted by the DHCP server.
default-gateway	Displays the IP address of the default gateway.
address	Displays the current IP address.
address source	Displays the BootP or DHCP client information. The possibilities for status returned are: • BootP Always • BootP or Last Address • BootP When Needed • Disabled • DHCP Always • DHCP or Last Address • DHCP When Needed

Displaying system information

Use this procedure to display detailed system information for the switch or stack.

Procedure

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

Displaying consolidated system information

Use this procedure to display consolidated information about the system.

Procedure

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

Displaying verbose system information

Use this procedure to display a verbose view of system information for a switch or stack.

Procedure

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

Displaying switch technical information

Use this procedure to display detailed technical information about system status, hardware, software, and switch operation

Procedure

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

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

Enabling feature license files

With the following procedures, you can copy the software license file to your switch and display or clear the existing license information:

Copying a software license file to the switch

Use this procedure to copy the features software license file from a TFTP server to your switch.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   copy tftp license <A.B.C.D> <WORD>
   ```
3.

Next steps

After you copy the license to the switch, you must perform a reboot to activate the license.

Note:

The software license is copied to NVRAM. If you reset the switch to default, this removes the software license from the switch. In this case, you must recopy the license file to the switch and reboot to reactivate the licensed features.

Variable definitions

The following table describes the parameters for the **`copy tftp license`** command.

Variable	Value
<A.B.C.D>	Specifies the TFTP server address.
<WORD>	Specifies the software license filename on the TFTP server.

Viewing the software licenses on the switch

Use this procedure to display the existing software licenses on the switch.

Procedure

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

```
show license { <1-10> | all }
```

Variable definitions

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

Variable	Value
<1–10>	Specifies the license to be displayed.
all	Displays all licenses.

Deleting software licenses on the switch

Use this procedure to delete the existing software licenses on the switch.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   clear license { <1-10> | all }
   ```

Variable definitions

The following table describes the parameters for the **`clear license`** command.

Variable	Value
<1–10>	Specifies the license to be cleared.
all	Clears all licenses.

Displaying flash information

Use this procedure to view information about the number of writes or modifications on the FLASH device. You can display FLASH information on both single and stacked switches. You can also display FLASH information for a specific unit.

Procedure

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. At the command prompt, enter the following command:
   ```
   show flash history [unit <1-8>]
   ```

Note:

The Flash History does not record programming done from the diagnostics or bootloader.

Note:

If you use `show flash` without the `history` parameter, the system outputs a message indicating that only flash history is active.

Example

```
5650TD-PWR>enable
5650TD-PWR#config t
5650TD-PWR#show flash history
-------------------------------------------------------------------------------
FLASH Write History :
-------------------------------------------------------------------------------
Section                    Number of writes
-------------------------------------------------------------------------------
Diagnostics Image:           0
Primary Image:               0
Secondary Image:             0
Config Area 1:               10
Config Area 2:               0
Auxiliary Config Area:       10
MCFG Block :                 29
Audit log Area :             109
-------------------------------------------------------------------------------
* Number of minimum guaranteed writes: 100 000
-------------------------------------------------------------------------------
5650TD-PWR#
```

Variable definitions

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

Variable	Value
history	Displays the flash writes and erase history.
unit <*1–8*>	Specifies a specific switch unit within a stack for which to display flash memory information.
Note: For a stack environment, if you do not specify a unit number with the `show flash` command, flash memory information for all switches within the stack is displayed.	

Configuring EDM inactivity timeout

Use this procedure to configure the EDM inactivity timeout on the switch.

About this task

You can configure the period of time after which an EDM session expires. The default period is 15 minutes (900 seconds). The setting does not affect current open sessions. The new setting applies only after logout and for future sessions.

Procedure

1. Enter Global Configuration mode:
   ```
   enable
   configure terminal
   ```
2. At the command prompt, enter the following command:
   ```
   edm inactivity-timeout <30–65535>
   ```
3. To set the inactivity timeout to its default value, enter the following command:
   ```
   [no] [default] edm inactivity-timeout
   ```
4. To display the EDM inactivity timeout value, enter the following command:
   ```
   show edm inactivity-timeout
   ```

Example

```
5650TD-PWR>enable
5650TD-PWR#config t
5650TD-PWR<config>#edm inactivity-timeout 300
5650TD-PWR<config>#show edm inactivity-timeout

EDM inactivity-timeout : 30
5650TD-PWR<config>#
```

Variable definitions

The following table describes the parameters for the **`edm inactivity-timeout`** command.

Variable	Value
<30–65535>	Specifies the timeout value in seconds. DEFAULT: 900

Variable	Value
[no]	Restores the EDM inactivity timeout to default value.
[default]	Restores the EDM inactivity timeout to default value

Chapter 9: Configuring and testing ports using ACLI

Use the procedures in this section to configure port features such as the port speed, duplex operation, autonegotiation settings, and autotopology.

Configuring Custom Autonegotiation Advertisements

Use the following procedures to configure Custom Autonegotiation Advertisement (CANA).

Custom Autonegotiation Advertisement (CANA) customizes the capabilities that are advertised. It also controls the capabilities that are advertised by the Avaya Ethernet Routing Switch 5000 Series as part of the auto-negotiation process.

Configuring CANA

Use this procedure to configure CANA.

Procedure

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

Variable definitions

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

Variable	Value
10–full	Advertises 10Mbps full-duplex.
10–half	Advertises 10Mbps half-duplex.
100–full	Advertises 100Mbps full-duplex.

Variable	Value
100–half	Advertises 100Mbps half-duplex.
1000–full	Advertises 1000Mbps full-duplex.
asymm-pause-frame	Advertises use of asymmetric pause frames half-duplex.
none	Specifies not to advertise anything during auto-negotiation.
pause-frame	Advertises use of pause frames.
port	Specifies the port or list of ports.

Displaying the current autonegotiation advertisements

Use this procedure to display the current autonegotiation advertisements.

Procedure

1. Log on to the User EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show auto-negotiation-advertisements [port <portlist>]
   ```

Variable definitions

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

Variable	Value
port <portlist>	Specifies the port or list of ports for which you want the current auto-negotiation advertisements displayed.

Setting the port speed

Use this procedure to set the speed of the port.

Procedure

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   speed [port <portlist>] {10 | 100 | 1000 | 10000 | auto}
   ```

Variable definitions

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

Variable	Value
port<*portlist*>	Specifies the port numbers for which to configure the speed. Enter the port numbers you want to configure. **Note:** If you omit this parameter, the system uses the port number you specified in the interface command.
10|100|1000|10000|auto	Sets speed to: • 10 means 10 Mbps • 100 means 100 Mbps • 1000 means 1000 Mbps or 1 Gbps • 10000 means 1000 Mbps or 10 Gbps • auto means autonegotiation default speed [port <*portlist*>] sets the speed of the port to the factory default speed.

Setting the port duplex operation

Use this procedure to specify the duplex operation for a port.

Procedure

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

```
duplex [port <portlist>] {full | half | auto}
```

Variable definitions

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

Variable	Value
port<*portlist*>	Specifies the port numbers for which to reset the duplex mode. Enter the port number you want to configure. The default value is autonegotiation. **Note:** If you omit this parameter, the system uses the port number you specified in the interface command.
full | half | auto	Sets duplex to: • full means full-duplex mode • half means half-duplex mode • auto means autonegotiation **Note:** Enabling/disabling autonegotiation for **speed** also enables/disables it for **duplex** operation. When you set the duplex mode for autonegotiation, ensure that the other side of the link is also set for autonegotiation. default duplex [port <*portlist*>] sets the duplex operation for a port to the factory default duplex value.

Displaying interfaces

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

About this task

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

Procedure

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

```
show interfaces [admin-disabled | admin-enabled | gbic-info |
link-down | link-up | names | verbose] [<portlist>]
```

Variable definitions

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

Variable	Value
admin-disabled	Display the interfaces with administration disabled.
admin-enabled	Display the interfaces with administration enabled.
gbic-info	Display the gbic details.
link-down	Display the interfaces with link down.
link-up	Display the interfaces with link up.
names	Display the interface names.
verbose	Display the port status information for various applications.
<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.

About this task

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 the User EXEC mode in ACLI.
2. At the command prompt, enter the following command:

```
show interfaces <portlist> config
```

Variable definitions

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

Variable	Value
<portlist>	Specifies the ports that you want to display.

Enabling or disabling Autotopology

Use this procedure to enable, disable, or reset the Autotopology protocol.

About this task

Autotopology enables a network management system (NMS) to reconstruct the network topology by collecting topology tables from each device that implements the autotopology network management module (NMM) behavior. NMM behavior is comprised of two activities:

- listening for SynOptics Network Management Protocol (SONMP) packets that are used to construct the topology table
- generating SONMP packets that other NMMs are listening for

The switch sends out two types of multicast packets every 10 seconds to all forwarding ports: Flatnet hello and Segment hello. It listens for only one type of multicast, Flatnet hello. The SONMP packets received are used to construct a topology table. The switch supports a maximum of 100 NMM topology table entries and 50 bridge topology table entries.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to enable Autotopology:
   ```
   autotopology
   ```
3. At the command prompt, enter the following command to disable Autotopology:
   ```
   no autotopology
   ```
4. At the command prompt, enter the following command to reset Autotopology to the factory default:
   ```
   default autotopology
   ```

Displaying Autotopology settings

Use this procedure to display the global autotopology settings.

Procedure

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

Displaying the Autotopology nmm table

Use this procedure to display the Autotopology network management module (NMM) table.

Procedure

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

Configuring flow control

Use this procedure to control the traffic rates on ports during congestion.

Procedure

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   flowcontrol [port <portlist>] {asymmetric | symmetric | auto | disable}
   ```

Variable definitions

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

Variable	Value
port<*portlist*>	Specifies the port numbers to configure for flow control.
asymmetric | symmetric | auto | disable	Sets the mode for flow control: • asymmetric means PAUSE frames can only flow in one direction. • symmetric means PAUSE frames can flow in either direction. • auto sets the port to automatically determine the flow control mode. • disable disables flow control on the port. DEFAULT: auto no flowcontrol [port <*portlist*>] disables flow control. default flowcontrol [port <*portlist*>] set the flow control to auto, which automatically detects the flow control.

Note:

If you omit either of these parameters, the system uses the ports you specified in the interface command but only those ports that have speed set to 1000/full.

Rate limiting configuration

The rate limiting feature allows you to configure the threshold limits for broadcast and multicast packets ingressing on a port for a given time interval. The ERS 5000 Series drops packets received above the threshold value if the traffic ingressing on the port exceeds the threshold.

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 ingress rate of those packet types to not exceed a specified percentage of the total available bandwidth or a specified number of packets per second.

Rate Limiting counts packets from the beginning of each second. When the number of packets reaches the value of the rate limit, all remaining packets are dropped until the end of the

second. As a result, the packets are not evenly distributed over the course of a second. For this reason, rate limiting utilization counters/calculations can appear to be inaccurate.

Note:

Rate Limiting behaves differently when the egress (out) port speed is less than the ingress (in) port speed.

When rate limiting is enabled on an ingress port and the egress port operates at a slower speed, traffic is sent to the egress port at the ingress port's (wire) speed. Egress rate limiting is done through a token bucket, and is not averaged over each second. Once the token bucket is full, traffic is dropped, as indicated in the *Dropped on no Resources* counter. When rate limiting is enabled on an ingress port, this behavior can have an effect on unicast packets.

Clarification of behavior:

Rate limit counts packets on the ingress port until the limit is reached and then drops everything until the end of the second. On a 1 Gbps ingress port, the first 10% of the 1Gb (100Mb) is allowed in the first tenth of the second and sent to the 100Mbps egress port. However, the 100Mbps port cannot handle 100Mb in a tenth of a second, as it can only handle 10Mb in a tenth of a second, and the rest is dropped.

Note:

If a packet with an unknown destination MAC is received (including during a FDB ageout) and rate limiting is set for either packet type of broadcast or both (broadcast and multicast), the rate limiting feature counts the unknown unicast packets in the same way as the broadcast packets.The system drops (filters) these unknown unicast packets.

Note:

Note the actual traffic received rate in the following scenario:

- rate-limiting is performed at 10% (or by setting any percent value threshold)
- the speed ratio between the inbound port and the client port is 10:1 (for example 10 Gbps inbound link and 1 Gbps client port link)
- inbound broadcast or multicast traffic throughput on the inbound link is more than 10% of the link-rate speed

The client port will receive 0.1 * (inbound traffic rate) and not the expected 1 Gbps broadcast or multicast traffic.

Example:

- inbound port link rate = 10Gbps, client outbound link rate = 1 Gbps, rate-limiting set to both at 10%
- inbound traffic rate = 3 Gbps broadcast traffic

The actual client traffic received rate = (0.1 * 3 Gbps) and not the expected 1 Gbps.

Displaying rate-limit configuration

Use this procedure to display the rate-limit configuration.

Procedure steps

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

```
show rate-limit
```

Variable definitions

The following table outlines the parameters of the **`show rate-limit`** command.

Table 2: show rate-limit parameters

Variable	Value
Port	Specifies the switch port numbers that correspond to the field values in that row of the screen (for example, the field values in row 2 apply to switch port 2). Note that the values applied in the Switch or Stack row (last 2 rows) affect all standalone switch ports or all switch ports in a stack.
Packet Type	Displays the packet type selected for rate-limiting or viewing. • Both — both multicast and broadcast packet types • Multicast • Broadcast Default value is Both.
Limit	Displays the percentage of port bandwidth allowed for forwarding the packet types specified in the Packet Type field. When the threshold is exceeded, any additional packets (specified in the Packet Type field) are discarded. Range is None, 1% to 10%. Default value is None. **Note:** Rate-limiting is disabled if this field is set to None. This allows you to select and view the percentage of specific packet types present in the network, without inadvertently limiting the forwarding rate.
Last 5 Minutes	Specifies the percentage of packets (of the type specified in the Packet Type field) received by the port in the last 5 minutes. This field provides a running average of network activity and is updated every 15 seconds.

Variable	Value
	Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.
Last Hour	Specifies the percentage of packets (of the type specified in the Packet Type field) received by the port in the last hour. This field provides a running average of network activity and is updated every 5 minutes. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.
Last 24 Hours	Specifies the percentage of packets (of the type specified in the Packet Type field) received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.

Configuring rate limiting

Use this procedure to configure rate limiting for either multicast or broadcast traffic, or both.

Procedure steps

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

   ```
   rate-limit [port <portlist>] {multicast | broadcast | both}
   {<0-10> | percent <0-10> | pps <0-262143>}
   ```

3. To disable rate limiting, enter the following command:

   ```
   no rate-limit [port <portlist>]
   ```

4. To restore the rate limiting to the default setting, enter the following command:

   ```
   default rate-limit [port <portlist>]
   ```

Variable definitions

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

Variable	Value
<portlist>	Specifies the port numbers on which to configure rate limiting.

Variable	Value
	Note: If you omit this parameter, the system uses the port number(s) you specified in the **interface** command
multicast | broadcast | both	Specifies the type of traffic for which to apply rate limiting: • multicast — applies rate limiting to multicast packets • broadcast — applies rate limiting to broadcast packets • both — applies rate limiting to both multicast and broadcast packets
percent <0–10> | pps <0–262143>	Specifies the mode for setting the rates f the incoming traffic: • percent <0–10> — enter an integer from 1 to 10 to set the rate-limiting percentage • pps <0–262143> — enter an integer from 1 to 262143 to set the rate-limiting packets per second For 10 Gbps links, the default value for limiting both broadcast and multicast is 10 percent. When using pps mode, the limit on 10 Gbps links cannot be configured to a value under 1000.

Note:

The rate-limit parameter of the ERS 5000 can be expressed as a percentage of total traffic. (ERS 5000 supports multicast/broadcast storm control as either a percentage or packets per second.)

When measuring the broadcast rate limit as a percentage, the rate limiting feature calculation is based on packets that are a fixed (not measured) average packet size of 500 bytes, rather than octets. To obtain the actual value, use the following equation (the average packet size is 500 bytes):

(Line speed (bit/sec) / average packet size x 8) X (Rate Limit / 100) = Packets per second

Chapter 10: Managing Power Over Ethernet (PoE) using ACLI

Setting the method to detect power devices

Set the method the Ethernet Routing Switch 5000–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 [unit <1–8>] {802dot3af |
802dot3af_and_legacy }
```

Variable definitions

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

Variable	Value
unit <1–8>	Specifies the unit in the stack to set the detection mode.
802dot3af | 802dot3af_and_legacy	Sets the detection method the switch uses to detect power needs of devices connected to the front ports: • 802dot3af • 802dot3af_and_legacy DEFAULT: 802dot3af_and_legacy

Variable	Value
	Important: Ensure that the power detection method you choose for the ERS 5000–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 5000–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 [unit <1-8>] {<1-99>}
   ```

Variable definitions

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

Variable	Value
unit <1–8>	Specifies the unit in the stack to set the detection mode.
<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 5000–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 the current PoE configuration

Display the current PoE configuration of the Ethernet Routing Switch 5000–PWR and settings for each PoE port.

Procedure

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

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

Example

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

```
5650TD-PWR#enable
5650TD-PWR+#show poe-main-status
PoE Main Status - Stand-alone
---------------------------
Available DTE Power        : 350 Watts
DTE Power Status           : Normal
DTE Power Consumption      : 0 Watts
```

```
DTE Power Usage Threshold  : 80 %
PD Detect Type             : 802.3af and Legacy
Power Supply 1             : AC-DC-48V-600W
Power Supply 2             : Unavailable
Power Status               : 1- OK 2- 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 User Exec command mode.
2. At the command prompt, enter the following command:

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

Example

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

```
5650TD-PWR#show poe-port-status
          Admin   Current                Limit
Port  Status  Status    Classification (Watts)   Priority----  ------- ------
-------------- ------    --------
1     Enable  Detecting   0              16        Low
2     Enable  Detecting   0              16        Low
3     Enable  Detecting   0              16        Low
```

```
4     Enable  Detecting   0              16        Low
5     Enable  Detecting   0              16        Low
6     Enable  Detecting   0              16        Low
7     Enable  Detecting   0              16        Low
8     Enable  Detecting   0              16        Low
9     Enable  Detecting   0              16        Low
10    Enable  Detecting   0              16        Low
11    Enable  Detecting   0              16        Low
12    Enable  Detecting   0              16        Low
13    Enable  Detecting   0              16        Low
14    Enable  Detecting   0              16        Low
15    Enable  Detecting   0              16        Low
16    Enable  Detecting   0              16        Low
17    Enable  Detecting   0              16        Low
18    Enable  Detecting   0              16        Low
19    Enable  Detecting   0              16        Low
----More (q=Quit, space/return=Continue)----
```

Variable definitions

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

Variable	Value
port <*portlist*>	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 User Exec command mode.
2. At the command prompt, enter the following command:
   ```
   show poe-power-measurement [port <portlist>]
   ```

Example

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

```
5650TD-PWR#enable
5650TD-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
port <*portlist*>	Enter the ports for which you want to display the power measurements. If you omit this parameter, the system displays all ports.

Disabling or enabling port power

Use this procedure to disable or enable Power Over Ethernet to a port.

Procedure

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command to disable Power Over Ethernet to a port:

   ```
   poe poe-shutdown [port <portlist>]
   ```

3. At the command prompt, enter the following command to enable Power Over Ethernet to a port:

   ```
   no poe poe-shutdown [port <portlist>]
   ```

Variable definitions

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

Variable	Value
port<*portlist*>	Specifies the ports for which PoE is enabled or disabled. **Note:** If you omit this parameter, the system uses the port number you specified in the interface command.

Setting port power priority

Use this procedure to set the port power priority.

Procedure

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   poe poe-priority [port <portlist>] {critical | high | low}
   ```

Variable definitions

The following table describes the parameters for the **poe-priority** command.

Variable	Value
port<*portlist*>	Specifies the ports for which to set the priority. **Note:** If you omit this parameter, the system uses the port number you specified in the interface command.
low | *high* | *critical*	Specifies the PoE priority for the port.

Setting power limit for channels

Use this procedure to set the power limit for channels.

Procedure

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   poe poe-limit [port <portlist>] <3-16>
   ```

Variable definitions

The following table describes the parameters for the **poe-limit** command.

Variable	Value
port<*portlist*>	Specifies the ports for which to set the limit. **Note:** If you omit this parameter, the system uses the port number you specified in the interface command.
<*3–16*>	Specifies the power range limit from 3 to 16 Watts.

Chapter 11: Updating switch software using ACLI

Use the procedures in this section to update the switch software, which is a necessary part of switch configuration and maintenance.

Before you begin

- The switch must be assigned a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is present on the network that is accessible by the switch and that has the desired software version loaded.
- If you change the switch software with software stored on a USB mass storage device, ensure that the mass storage device has the desired software version loaded on it and is inserted into the front panel USB port.

Changing switch software

Use this procedure to specify the download target image and change the software version running on the switch.

About this task

You can update either active image or non-active image. Once the image download is done, the unit resets and restarts with the new image regardless of the value of the Next Boot image indicator. In case of image download without reset, the new image in the flash will be the Next Boot image.

The software download process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process. Depending on network conditions, this process can take up to 10 minutes.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

```
download [usb | sftp | tftp] [address <A.B.C.D> | <WORD>]
[primary | secondary] {image <image_name> | image—if—newer
<image_name> | diag <image_name>} [no-reset]
```

3. Press `Enter`.

Example

The switch is not operational during the download process. You can track the progress of the download process by observing the front panel LEDs.

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

The following shows an example of this message.

```
Downloading Image [/]
Saving Image [-]
Finished Upgrading Image
```

Variable definitions

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

Note:

The IPv6 parameter is valid only for switches that support IPv6.

Variable	Value
usb | tftp | sftp	Specifies the software download source. USB is performed using a USB mass storage device. TFTP is performed using a TFTP server. SFTP is performed using a SFTP server.
address<*A.B.C.D*> | <*WORD*>	Specifies the IP or IPv6 address of the TFTP or SFTP server to be used. The address parameter is optional and if omitted the switch defaults to the TFTP server specified by the `tftpserver` command unless software download is to take place using a USB mass storage device.
primary | secondary	Specifies the image to download: primary or secondary.
image <*image_name*>	Specifies the name of the software image to be downloaded from the TFTP server.

Variable	Value
image—if—newer <*image_name*>	Specifies the name of the software image to be downloaded from the TFTP server if newer than the currently running image.
diag <*image_name*>	Specifies the name of the diagnostic image to be downloaded from the TFTP server.
no-reset	Stops the switch from resetting after the software download is complete.

Note:

The `image`, `image-if-newer`, and `diag` parameters are mutually exclusive and only one can be executed at a time.

Toggling the Dual Agent next boot image

Use this procedure to toggle the next boot image.

About this task

The Next Boot image in Dual Agent is an agent image that is stored in the flash memory to be used for the next boot. In Dual Agent, there are two agent images in the flash memory, but only one image is assigned as the Next Boot image at a time.

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

You can change the Next Boot image at any time. The Next Boot image indicator (a value to indicate which agent image in the flash memory is used in the next boot) is stored in the NVRAM. This value, combined with other factors in the stack discovery process, determines which Dual Agent image the switch uses.

Procedure

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

   Note:

   You must restart the switch or stack after this command to use the next boot image as the new primary image.

Displaying agent images

Use this procedure to show the agent image information for agent images stored in the flash memory.

Procedure

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

Selecting the Dual Agent secondary boot image

Use this procedure to use the secondary boot image.

Procedure

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

Note:
The switch or stack will restart automatically with the new image.

Chapter 12: Shutting down and resetting a switch using ACLI

Use the procedures in this section to use the `shutdown` command for safely shutting down a switch or stack and the `reload` command to configure remote devices.

About this task

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

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

The `reload` command differs from the `shutdown` command in that the configuration is not explicitly saved after the command is issued. This means that any configuration changes must be explicitly saved before the switch or stack reloads. The `reload` command does temporarily disable auto-save functionality until the reload occurs. Cancelling the reload returns auto-save functionality to any previous setting.

Shutting down the switch

Use this procedure to shut down a switch or stack.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
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 parameter.

Reloading remote devices

Use this procedure to reload a switch or stack.

About this task

You can use the reload command 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 reestablish connectivity.

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 the Privileged EXEC mode in ACLI
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:

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.

```
reload force minutes-to-wait 30
```

Execute dynamic switch configuration commands. The commands take effect immediately and are not saved to NVRAM.

Test your configuration changes. If problems occurred, when the 30 minute countdown expires the switch reboots and loads the previous configuration. If no problems occurred, and switch connectivity is maintained, you can perform one of the following tasks before the 30 minute countdown expires.

Save the new configuration.

```
copy config nvram
```

Cancel the previous reload command.

```
reload cancel
```

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 parameter.

Chapter 13: Configuring a Virtual Fabric using ACLI

Use the procedures in this section to configure a Virtual Fabric (stack) using ACLI. You can configure New Unit Quick Configuration, Auto Unit Replacement features, and Stack Forced Mode.

Stacking capabilities

You can use the Avaya Ethernet Routing Switch 5600 Series switches in either of the following configurations:

- stand-alone
- stack

The Avaya Ethernet Routing Switch 5600 Series switches have a built-in cascade port to stack up to eight units.

A stack can consist of any combination of Avaya Ethernet Routing Switch 5600 Series switches.

Important:

All units in the stack must use the same software version.

To set up a stack, perform the following procedure.

Procedure steps

1. Power down all switches.
2. Set the Unit Select switch in the back of the non base units to the off position.
3. Set the Unit Select switch in the back of the base unit to base position.
4. Ensure all the cascade cables are properly connected and screwed into the unit.
5. Power up the stack.

Stack monitor

You can create a stack with up to eight Avaya Ethernet Routing Switch 5600 Series switches.

Stack manager is responsible for the following functions that form and maintain a stack.

- Base unit selection.
- Unit discovery.
- Unit number assignment.
- Database exchange.
- Join stack handling.
- Programming the hardware for the stack to function as a system.

Stack manager also handles link events from the Hello module when a unit is added or removed from the stack. Based on the event, the stack manager again runs through the state machine to discover the newly added unit or change the stack configuration. Stack manager supports following stack configurations:

- Ring topology: All the units are connected as a ring.
- Upstream: All the non-base units are upstream to the base unit.
- Downstream: All the non-base units are downstream to the base unit.
- Up Down: Non base units are both upstream and downstream of the base unit.

Stack manager supports a maximum of eight switches in a stack. Although the design does not restrict the number of ports in a stack, Avaya recommends that the number does not exceed 400 ports.

Enabling or disabling Quick Configuration

Use the following commands to enable or disable Quick Configuration:

Before you begin

Quick Configuration requires a stack.

About this task

The new unit Quick Configuration can store a default configuration that applies to a new unit joining the stack.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. To enable Quick Configuration, enter the following command:
   ```
   quickconfig enable
   ```
3. To disable Quick Configuration, enter the following command:
   ```
   no quickconfig enable
   ```
4. To default Quick Configuration, enter the following command:
   ```
   default quickconfig
   ```

Next steps

Use the **`quickconfig start-recording`** command to record a default configuration that applies to new units joining the stack.

Recording a Quick Configuration

Use this procedure to record a Quick Configuration:

Before you begin

Quick Configuration requires a stack.

Quick Configuration must be enabled.

About this task

You can use the new unit Quick Configuration feature to create a default configuration that applies to any new unit joining the stack. You can record the default values for VLAN IDs, port speed, duplex mode, PVID, tagging, and spanning tree groups for the new unit without the need to reset the stack.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   quickconfig start-recording
   ```
3. Record your required Quick Configuration by entering one command on each line in ACLI. See the following example.

   Important:

   The first two commands must be `enable` and `config term`, otherwise the configuration commands that follow do not apply.

Use `$` as a wildcard for the slot. The unit number is not known when a new unit joins a stack, so the wildcard can match any slot number.

To end the recording process enter a `.` on the last line in ACLI.

Example

The following example records a Quick Configuration for VLAN and port configurations that applies to a new unit joining a stack if Quick Configuration is enabled:

```
enable
config term
vlan port $/13-40 tag untagPvidonly
vlan create 10 name vlan_10 type port
vlan create 20 name vlan_20 type port
vlan members add 10 $/13-40
vlan members add 20 $/13-40
interface Ethernet $/13-34
speed 100
end
.
```

Enabling or disabling AUR

Use the following commands to enable or disable Auto Unit Replacement (AUR).

Before you begin

AUR requires a stack configuration

About this task

You can use the Auto Unit Replacement (AUR) feature to replace a unit in a stack and automatically restore the saved configuration image from the old unit to the new unit.

Procedure

1. Log on to the 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 the following procedure to view the AUR configuration.

Before you begin

AUR requires a stack configuration.

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
   ```

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
   ```

Saving or restoring AUR configurations

Use the following commands to save or restore a configuration.

Before you begin

AUR requires a stack configuration.

About this task

You can manually save or restore an AUR configuration to a non-base unit.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. To save a configuration, enter the following command:
   ```
   stack auto-unit-replacement config save unit <1-8>
   ```
3. To restore a configuration, enter the following command:
   ```
   stack auto-unit-replacement config restore unit <1-8>
   ```

Note:

You must enter a valid unit number of 1 to 8 to save or restore a configuration to a specific unit in a stack.

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.

Enabling or disabling AAUR

Use the following commands 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 AAUR, enter the following command:
   ```
   stack auto-unit-replacement-image enable
   ```
3. To disable AAUR, enter the following command:
   ```
   no stack auto-unit-replacement-image enable
   ```
4. To default AAUR, enter the following command:
   ```
   default stack auto-unit-replacement-image enable
   ```
   The default is enabled.

Displaying the AAUR configuration

Use the following procedure to view the AAUR configuration.

Before you begin

AAUR requires a stack configuration.

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-image
   ```

Enabling or disabling Stack Forced Mode

Use the following commands to enable or disable Stack Forced Mode.

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 the 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.

Next steps

Use the following command to display the current Stack Forced Mode configuration:

```
show stack forced-mode
```

Displaying Stack Forced Mode

Use the following procedure to view the Stack Forced Mode configuration.

Before you begin

Stack Forced Mode requires a stack configuration of two units.

Procedure

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

Chapter 14: Configuring the switch using EDM

Use the procedures in this section to configure your switch for the first time using Enterprise Device Manager (EDM).

Configuring Quick Start

Use the following procedure to configure the Quick Start setup mode using EDM.

About this task

You can use Quick Start to quickly setup a new switch or stack.

Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Quick Start**.
3. In the work area, click the **IP/Community/Vlan** tab.
4. In the **In-Band Switch IP Address** field, type a switch or stack IP address.
5. In the **In-Band Stack Subnet Mask** field, type a subnet mask.
6. In the **Default Gateway** field, type a gateway IP address.
7. In the **Read-Only Community String** field, type a community string. Re-type the community string in the verification field.
8. In the **Read-Write Community String** field, type a community string. Re-type the community string in the verification field.

   Note:

   For security, enter different community strings for Read-Only and Read-Write.
9. In the **Quick Start VLAN** field, type a VLAN ID ranging from 1 to 4094.
10. On the toolbar, click **Apply**.

Configuring out-of-band management

Use this procedure to configure the out-of-band management IP address, subnet mask, and default gateway.

About this task

When you physically connect Ethernet RJ-45 management port for standalone switch or stack to your network and assign an IP address to the port, you can use the management port to access the switch or stack using Telnet, SSH, SNMP, HTTP, and HTTPS.

Note:

The out-of-band management IP address must be different than the switch or stack in-band management IP address.

Procedure

1. From the navigation pane, double-click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Switch/Stack**.
4. In the Switch/Stack work area, click the **Management IP** tab.
5. To configure out-of-band management parameters for a switch, double-click table cells as required.
6. On the toolbar, click **Apply**.
7. On the toolbar, you can click **Refresh** to verify the out-of-band management configuration.

Variable definitions

Variable	Value
Indx	Indicates a stack switch unit, for which to configure an out-of-band management IP address. Values range from 1 to 8. For a stack environment, an **Indx** value of 1 specifies the base unit. For a standalone switch, the **Indx** value is 1.

Variable	Value
IpMgmtAddress	Specifies an out-of-band management IP address for the selected switch. DEFAULT: 0.0.0.0
IpMgmtNetMask	Specifies the subnet mask associated with the out-of-band management IP address. DEFAULT: 0.0.0.0
IpMgmtGateway	Specifies the IP address for the out-of-band management default gateway. DEFAULT: 0.0.0.0 **Important:** The out-of-band management default gateway takes precedence over the in-band management default gateway.

Configuring remote access

Use the following procedure to configure remote access for a switch or stack.

Procedure

1. From 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 Access Setting section, select a value from the **Access** list.
5. In the Telnet 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.

   Note:

   SSH Remote Access is only available in secure software builds.
10. In the SSH Remote Access Setting section, select a value from the **Use List** list.

Note:

SSH Remote Access is only available in secure software builds.

11. On the toolbar, click **Apply**.

Variable Definitions

The data in the following table describes configuring remote access for a switch or stack using EDM.

Variable	Value
Telnet Remote Access Setting	Specifies the remote access settings for telnet sessions. If you need to describe a series of choices for the field, use an unordered list as follows: • **Access**: allows or denies telnet access to the switch or stack. • **Use List**: Enables (Yes) or disables (No) the use of remote access list Telnet information.
SNMP Remote Access Setting	Specifies the remote access settings for SNMP. If you need to describe a series of choices for the field, use an unordered list as follows: • **Access**: allows or denies SNMP access to the switch or stack. • **Use List**: Enables (Yes) or disables (No) the use of remote access list SNMP information.
Web Page Remote Access Setting	Specifies the remote access settings for Web Page. If you need to describe a series of choices for the field, use an unordered list as follows: • **Use List**: Enables (Yes) or disables (No) the use of remote access list web page information.
SSH Remote Access Setting	Specifies the remote access settings for SSH.

Variable	Value
	Note: SSH is only available in secure software builds. If you need to describe a series of choices for the field, use an unordered list as follows: • **Access**: allows or denies SSH access to the switch or stack. • **Use List**: Enables (Yes) or disables (No) the use of remote access list SSH information.

Run IP Office script configuration

The Run IP Office script executes a set of commands in either a fully automated or user prompted configuration on ACLI or EDM. In a fully automated or default mode, the scripts are executed with the predefined default values. In a user-prompted or the verbose mode, you can use the script to modify the default values.

You do not need access rights to execute the script. The script is available in both standalone and stacking mode. In stacking mode, you must execute the script from the base unit.

Note:

The script must be executed on a switch with default settings. If you execute the script on a switch that is already configured, you can encounter script failure or an incomplete configuration.

Table 3: Default parameters for Run IP Office 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
Data VLAN Gateway IP/mask	255.255.255.0
IP Route to Gateway Modem-Router (Internet/WAN)	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)	Gateway Modem-Router port

Configuring with IP Office Script

Use the following procedure to configure parameters using the IP Office Script.

Note:

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

Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Run Script**.
3. In the work area, click the **IP Office Script** tab.
4. In the **Run Script Mode** section, click a radio button.
   If you select **default**, the parameters are automatically configured. If you select **verbose**, proceed with the following steps to modify the parameters in verbose mode.
5. In the **Voice VLAN Id** field, type a value.
6. In the **Voice VLAN Gateway** field, type a value.
7. In the **Voice VLAN Gateway Mask** field, type a value.
8. In the **Data VLAN Id** field, type a value.
9. In the **Data VLAN Gateway** field, type a value.
10. In the **Data VLAN Gateway Mask** field, type a value.
11. In the **IP Route to Gateway Modem-Router** field, type a value.
12. In the **IP Office Call-Server** field, type a value.
13. In the **IP Office File-Server** field, type a value.
14. Click **Apply**.

IP Office Script field descriptions

Name	Description
Run Script Mode	Specifies to run the script either in default or verbose mode.
Voice VLAN Id	Specifies the voice VLAN ID. By default, the voice VLAN ID is 42.
Voice VLAN Gateway	Specifies the Voice VLAN Gateway IP Address. By default, the voice VLAN gateway IP address is 192.168.42.254.
Voice VLAN Gateway Mask	Specifies the voice VLAN gateway IP mask address. By default, the voice VLAN gateway IP mask address is 255.255.255.0. The default subnet mask created by the run IP Office script supports a maximum of 250 hosts. You can change the subnet mask to 255.255.254.0 to allow 510 hosts for each subnet using the verbose mode.
Data VLAN ID	Specifies the data VLAN ID. By default, the data VLAN ID is 44.
Data VLAN Gateway	Specifies the data VLAN Gateway. By default, the data VLAN Gateway is 192.168.44.254.
Data VLAN Gateway Mask	Specifies the data VLAN Gateway Mask. By default, the data VLAN Gateway Mask is 255.255.255.0.
IP Route to Gateway Modem-Router	Specifies the IP Route to gateway modem and router. By default, the IP address is 192.168.44.2.
IP Office Call-Server	Specifies the IP Office call server IP address. By default, the call server IP address is 192.168.42.1.
IP Office File-Server	Specifies the IP Office file server IP address. By default, the file server IP address is 192.168.42.1.

Name	Description
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. • passed—the selected operation succeeded. • failed—the selected operation failed.

Configuring with ADAC Script

Use the following procedure to configure ADAC parameters for the switch.

Note:

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

Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Run Script**.
3. In the work area, click the **ADAC Script** tab.
4. In the Verbose section, in the **Data VLAN ID** field, type the data VLAN ID.
5. Select **Management VLAN flag** if you want the data VLAN as the management VLAN.
6. In the **Data VLAN Gateway** dialog box, type the data VLAN Gateway IP address.
7. In the **Data VLAN Gateway Mask** dialog box, type the data VLAN Gateway mask address.
8. In the **Management IP address** dialog box, type the management IP address.
9. In the **Management IP Mask** dialog box, type the management IP mask.
10. In the **Default IP Route** dialog box, type the default IP route address.
11. In the **Voice VLAN Id** dialog box, type the voice VLAN ID.

12. In the **Voice VLAN Gateway** dialog box, type the IP address.
13. In the **Voice VLAN Gateway Mask** dialog box, type the IP mask address.
14. In the **LLDP Call-Server** dialog box, type the LLDP call server IP address.
15. In the **LLDP File-Server** dialog box, LLDP file server IP address.
16. (Optional) Select the **Uplink trunk flag** to link ADAC uplink port as a member of MLT trunk.
17. Click the **ADAC Uplink Ports** ellipsis (...).
18. From the ADAC Uplink Ports, select the uplink ports and then, click Ok.
19. Click the **ADAC Call Server Ports** ellipsis (...).
20. From the ADAC Call Server ports, select the call serevr ports and then, click Ok.
21. Click the **ADAC Telephony Ports** ellipsis (...).
22. From the ADAC Telephony Ports, select the telephony ports and then, click Ok.
23. Click **Apply**.

ADAC Script field descriptions

Name	Description
Run Script Mode	Specifies to run the script in verbose mode and it is selected by default.
Data VLAN Id	Specifies the data VLAN ID. The value ranges from 1 to 4096.
Management VLAN flag	Specifies data VLAN ID as Management VLAN. This is optional.
Data VLAN Gateway	Specifies the data VLAN gateway IP address.
Data VLAN Gateway Mask	Specifies the data VLAN gateway mask IP address.
Management IP address	Specifies the management IP address.
Management IP Mask	Specifies the management IP mask address.
Default IP Route	Specifies the default IP route.
Voice VLAN Id	Specifies the voice VLAN ID. By default, the voice VLAN ID is 42.

Name	Description
Voice VLAN Gateway	Specifies the Voice VLAN Gateway IP Address. By default, the voice VLAN gateway IP address is 192.168.42.254.
Voice VLAN Gateway Mask	Specifies the voice VLAN gateway IP mask address. By default, the voice VLAN gateway IP mask address is 255.255.255.0.
LLDP Call-Server	Specifies the LLDP call server IP address.
LLDP File-Server	Specifies the LLDP file server IP address.
Uplink trunk flag	Links the ADAC uplink port to the MLT trunk.
ADAC Uplink Ports	Specifies the ADAC uplink ports. A maximum of 50 ports are supported.
ADAC Call Server Ports	Specifies the ADAC call server ports. A maximum of 50 ports are supported.
ADAC Telephony Ports	Specifies the ADAC telephony ports. A maximum of 50 ports are supported.
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. • passed—the selected operation succeeded. • failed—the selected operation failed.

Configuring with LLDP Script

Use the following procedure to configure LLDP parameters for the switch.

Note:

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

Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Run Script**.
3. In the work area, click the **LLDP Script** tab.
4. In the Mode work area, by default, verbose is selected in the **Run Script Mode** dialog box.
5. In the Verbose work area, type the data VLAN ID in the **Data VLAN Id** dialog box.
6. Select **Management VLAN flag** if you want the data VLAN as the management VLAN.
7. In the **Data VLAN Gateway** dialog box, type the data VLAN Gateway IP address.
8. In the **Data VLAN Gateway Mask** dialog box, type the data VLAN Gateway mask address.
9. Click the **Data VLAN Uplink Ports** ellipsis (...) and select ports.
10. In the **Management IP address** dialog box, type the management IP address.
11. In the **Management IP Mask** dialog box, type the management IP mask.
12. In the **Default IP Route** dialog box, type the default IP route address.
13. In the **Voice VLAN Id** dialog box, type the voice VLAN ID.
14. In the **Voice VLAN Gateway** dialog box, type the IP address.
15. In the **Voice VLAN Gateway Mask** dialog box, type the IP mask address.
16. In the **LLDP Call-Server** dialog box, type the LLDP call server IP address.
17. In the **LLDP File-Server** dialog box, LLDP file server IP address.
18. Click **Apply**.

LLDP Script field descriptions

Name	Description
Run Script Mode	Specifies to run the script in verbose mode and it is selected by default.
Data VLAN Id	Specifies the data VLAN ID. The value ranges from 1 to 4096.
Management VLAN flag	Specifies data VLAN ID as Management VLAN. This is optional.

Name	Description
Data VLAN Gateway	Specifies the data VLAN gateway IP address.
Data VLAN Gateway Mask	Specifies the data VLAN gateway mask IP address.
Data VLAN Uplink Port	Specify the ports for Data VLAN uplink.
Management IP address	Specifies the management IP address.
Management IP Mask	Specifies the management IP mask address.
Default IP Route	Specifies the default IP route.
Voice VLAN Id	Specifies the voice VLAN ID. By default, the voice VLAN ID is 42.
Voice VLAN Gateway	Specifies the Voice VLAN Gateway IP Address. By default, the voice VLAN gateway IP address is 192.168.42.254.
Voice VLAN Gateway Mask	Specifies the voice VLAN gateway IP mask address. By default, the voice VLAN gateway IP mask address is 255.255.255.0.
LLDP Call-Server	Specifies the LLDP call server IP address.
LLDP File-Server	Specifies the LLDP file server IP address.
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. • passed—the selected operation succeeded. • failed—the selected operation failed.

Configuring system parameters

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

Procedure

1. From 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 **System** tab.
5. In the **sysContact** field, type the system administrator contact information.
6. In the **sysName** field, type the system name.
7. In the **sysLocation** field, type the system location.
8. To enable authentication traps, select the **Authentication Traps** check box.
   OR
   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 **StackInsertionUnitNumber** field, type a value.
12. To enable jumbo frames, select the **JumboFramesEnabled** check box.
    OR
    To disable jumbo frames, clear the **JumboFramesEnabled** check box.
13. To enable serial security, select the **SerialSecurityEnable** check box.
    OR
    To disable serial security, clear the **SerialSecurityEnable** check box.
14. To enable forced stack mode, select the **ForcedStackModeEnabled** check box.
    OR
    To disable forced stack mode, clear the **ForcedStackModeEnabled** check box.
15. To enable Quick Configuration, select the **QuickConfigEnable** check box.
    OR
    To disable Quick Configuration, clear the **QuickConfigEnable** check box.
16. In the **EdmInactivityTimeout** section, enter a value.
17. In the **MgmtStackIpAddress** section, enter an IPv4 address.
18. In the **StackIpv6MgmtAddress** section, enter an IPv6 address.
19. In the **StackIpv6MgmtNetMask** section, enter a netmask.
20. In the **Ipv6MgmtGateway** section, enter a gateway IPv6 address.
21. In the **BootMode** section, click a radio button.
22. On the toolbar, click **Apply**.

Variable definitions

The following information describes the system level configuration.

Variable	Value
sysDescr	Indicates the device specific information.
sysUpTime	Indicates the amount of time since the last system reboot.
sysObjectID	Indicates the system object identification number.
sysContact	Specifies the contact information for the system administrator. Value can include a name or email address.
sysName	Specifies a unique name to describe this system.
sysLocation	Specifies the physical location of this system.
AuthenticationTraps	Enables or disables authentication traps. • When enabled, SNMP traps are sent for all SNMP access authentications. • When disabled, no SNMP traps are received.
Reboot	Specifies the action to reboot the switch. • running — the switch remains running. • bootPrimary — reboots the switch with the Primary image. • bootSecondary — reboots the switch with the Secondary image.
AutoPvid	When enabled, a VLAN ID can be automatically assigned to any port.
stackInsertionUnitNumber	Specifies the unit number to assign to the next unit joining the stack. Values range from 0–8. **Important:** You can use this to manually specify a unit number to the next unit joining a stack. Once used, the value returns to 0, and auto unit numbering resumes. You cannot

Variable	Value
	edit the unit number of an existing stack unit.
JumboFramesEnabled	Enables or disables jumbo frames.
JumboFramesSize	Specifies the size of the jumbo frames. Value ranges from 1519 to 9216 bytes. DEFAULT: 9216
SerialSecurityEnable	Enables or disables the serial security feature.
ForcedStackModeEnabled	Enables or disables Forced Stack Mode.
QuickConfigEnable	Enables or disables Quick Configuration.
EdmInactivityTimeout	Specifies the timeout value in seconds. Value ranges from 30 to 65535. DEFAULT: 900
MgmtStackIpAddress	Specifies an out-of-band management IP address for the stack.
StackIpv6MgmtAddress	Specifies an out-of-band management IPv6 address for the stack.
StackIpv6MgmtNetMask	Sepcifies the subnet mask associated with the out-of-band management IP address.
Ipv6MgmtGateway	Specifies the management default gateway.
NextBootMgmtProtocol	Indicates the transport protocols to use after the next reboot.
CurrentMgmtProtocol	Indicates the current supported transport protocols.
BootMode	Specifies the use of BootP or DHCP server to assign an IPv4 address for the management VLAN at the next reboot. • other — read only • bootpDisabled — use the configured server IP address • bootpAlways — always use the BootP server • bootpWhenNeeded — use the BootP server when needed • bootPOrLastAddress — use the BootP server last used • dhcpAlways — always use the DHCP server

Variable	Value
	• dhcpWhenNeeded — use the DHCP server when needed • dhcpOrLastAddress — use the DHCP server last used
CurrentImageVersion	Indicates the switch version number of the agent image currently running.
NextBootDefaultGateway	Indicates the IP address of the default gateway for the agent to use on reboot.
CurrentDefaultGateway	Indicates the IP address of the default gateway that is currently in use.
NextBootLoadProtocol	Indicates the transport protocol that the agent uses to load the configuration information and agent image on reboot.
LastLoadProtocol	Indicates the transport protocol last used to load the configuration information and agent image.

Displaying unit information

Use this procedure to display information for a single unit on the switch.

Procedure

1. In the **Device Physical View**, select the unit.
2. From the navigation tree, double-click **Edit**.
3. From the Edit tree, click **Unit**.

Unit field descriptions

The following table describes the fields on the Unit tab.

Name	Description
Type	Specifies the type number.
Descr	Specifies the type of switch.
Ver	Specifies the version number of the switch.

Name	Description
SerNum	Specifies the serial number of the switch.
BaseNumPorts	Specifies the base number of ports.
TotalNumPorts	Specifies the total number of ports.

Displaying the PoE information for a unit

Use this procedure to display PoE information for a single unit.

Note:

You can only view PoE parameters by selecting a single unit.

Procedure

1. In the **Device Physical View**, select the unit.
2. From the navigation tree, double-click **Edit**.
3. From the Edit tree, click **Unit**.
4. Select the **PoE** tab.

PoE field descriptions

The following table outlines the parameters of the **PoE** tab.

Name	Description
Power	Displays the total power available to the Avaya Ethernet Routing Switch.
OperStatus	Displays the power state of the Avaya Ethernet Routing Switch • **on** • **off** • **faulty**
Consumption Power	Displays the power being used by the Avaya Ethernet Routing Switch.
UsageThreshold	Enables you to set a percentage of the total power usage of the Avaya Ethernet

Name	Description
	ROouting Switch based on which system sends a trap. **Note:** You must have the traps enabled (see NotificationControlEnable) to receive a power usage trap.
Notification Control Enable	Enables you to enable or disable sending traps if the switch's power usage exceeds the percentage set in the Usage Threshold field.
PowerDeviceDetectType	Enables you to set the power detection method that the switch uses to detect a request for power from a device connected to all ports on the switch: • **802.3af**. • **802.3afAndLegacySupport**

Configuring Asset ID

Use the following procedure to configure an Asset ID for a switch or stack.

Procedure

1. From 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, double-click a cell in the **AssetID** column for the unit you want to configure.
6. Type an Asset ID value in the **AssetID** field.
7. On the toolbar, click **Apply**.

Variable definitions

The following table describes configuring an Asset ID.

Variable	Value
Stack	Specifies the Asset ID of the stack.
Unit 1	Specifies the Asset ID of unit 1.
Unit 2	Specifies the Asset ID of unit 2.

Note:

You can specify an Asset ID of up to eight units.

Selecting the ACLI banner type

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

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Chassis**
4. In the Chassis work area, click the **Banner** tab.
5. In the **BannerControl** section, click a radio button.
6. Click **Apply**.

Variable definitions

The following table describes the variables associated with ACLI banner types.

Variable	Value
Static	Uses the predefined static banner.
Custom	Uses the previously set custom banner.
Disabled	Prevents the display of any banner.

Customizing the ACLI banner

Use this procedure to customize banner that is displayed on the Avaya Command Line (ACLI) Telnet screen.

Before you begin

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

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the Chassis work area, click the **Custom Banner** tab.
5. Select a row (switch), configure as required.
6. On the toolbar, click **Apply**.
7. On the toolbar, you can click **Refresh** verify the configuration.

Variable definitions

The following table describes the variables associated with customizing the ACLI banner.

Variable	Value
Type	Indicates whether the banner type is for a standalone (switch) or a stack (stack).
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.

Managing an ASCII configuration file

Use the following procedure to automatically download, manually download, or manually upload an ASCII configuration file.

About this task

An ASCII configuration file contains the switch configuration. You can download, store, or retrieve the ASCII configuration file from a TFTP server or USB device.

Procedure

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, click **File System**.
3. In the work area, click the **Ascii Config File** tab.
4. To transfer the configuration file using TFTP or SFTP, in the **TftpServerInetAddressType** field, click a radio button.
5. To transfer the configuration file using TFTP or SFTP, in the **TftpServerInetAddress** field, type the IP address of the TFTP server.
6. In the **AsciiConfigFilename** field, type the name of the configuration file.
7. To transfer the configuration file using USB, in the **UsbTargetUnit** field, type a value.

   Important:

   You must enter a value in the **UsbTargetUnit** field for TFTP or SFTP configuration file transfers.
8. To automatically download the configuration file, in the **AsciiConfigAutoDownload** field, click a radio button.
9. To manually download and retrieve the configuration file, in the **AsciiConfigManualDownload** field, click a radio button.
10. To manually upload specific application configurations, in the **Application** field, select the applications.
11. To manually upload and store the configuration file, in the **AsciiConfigManualUpload** field, click a radio button.

    Important:

    To manually upload specific applications only, you must select a Verbose upload option.
12. On the toolbar, click **Apply**.

13. To verify the status of the configuration file transfer, view the **AsciiConfigAutoDldStatus**, **AsciiConfigManualDldStatus**, or the **AsciiConfigManualUpldStatus** field.

Variable definitions

The following table describes managing an ASCII configuration file.

Variable	Value
TftpServerInetAddressType	Specifies the TFTP or SFTP server IP address type as IPv4 or IPv6.
TftpServerInetAddress	Specifies the TFTP or SFTP server IP address.
AsciiConfigFileName	Specifies the file name of the ASCII configuration file to download or upload.
UsbTargetUnit	Specifies the unit or server type. Values include: • 1 to 8 — units in a stack • 9 — standalone unit • 0 — TFTP server • 10 — SFTP server
AsciiConfigAutoDownload	Specifies if the ASCII configuration file is downloaded during boot. Values include: • disabled — Automatic downloading is disabled • useBootp — Use BootP to obtain TFTP server settings, the TFTPServerInetAddress is not used • useConfig — Use the TFTPServerInetAddress
AsciiConfigAutoDldStatus	Indicates the file transfer status. Values include: • InProgress — Download in progress, wait 2 minutes, and then click Refesh • Passed — Download completed successfully • Failed — Download failed

Variable	Value
AsciiConfigManualDownload	Specifies the manual file download method. Values include: • downloadNow — Download from the TFTP server • downloadFromUsb — Download from a USB storage device
AsciiConfigManualDldStatus	Indicates the file transfer status. Values include: • InProgress — Download in progress, wait 2 minutes, and then click Refesh • Passed — Download completed successfully • Failed — Download failed
Applications	Specifies the application configurations to transfer in Verbose mode.
AsciiConfigManualUpload	Specifies the manual file upload method. Values include: • uploadNow — Upload to the TFTP server • uploadToUsb — Upload to a USB storage device • uploadVerboseNow — Upload specific applications to the TFTP server • uploadVerboseToUsb — Upload specific applications to a USB storage device
AsciiConfigManualUpldStatus	Indicates the file transfer status. Values include: • InProgress — Download in progress, wait 2 minutes, and then click Refesh • Passed — Download completed successfully • Failed — Download failed

Saving the current configuration

Use the following procedure to configure Autosave or manually save the current configuration.

About this task

The current configuration is regularly saved to the flash memory if Autosave is enabled. You can use the following procedure to manually save the current configuration.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. In the work area, click the **Save Configuration** tab.
4. Select the **AutosaveToNvramEnabled** check box to enable automatically saving the configuration to flash memory (Autosave), or clear the check box to disable Autosave.
5. To manually save the current configuration, click the **copyConfigToNvram** radio button.
6. On the toolbar, click **Apply**.
7. On the toolbar, click **Refresh**.

Variable definitions

The following table describes saving the current configuration.

Variable	Value
AutosaveToNvramEnabled	Specifies if Autosave is enabled or disabled. If enabled (selected), the system automatically saves the configuration to the flash memory.
Action	Specifies the action you want to perform. • other — read only and default • copyConfigToNvram — manually saves the current configuration
Status	Indicates the current status.

Configuring SNTP

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

About this task

You can configure the switch clock to SNTP, configure the SNTP server IP addresses, and configure the SNTP synchronization intervals.

Procedure

1. From the navigation tree, double-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** field, click a radio button to select IPv4 or IPv6.
5. In the **PrimaryServerInetAddress** field, type the primary IP address.
6. In the **SecondaryServerInetAddressType** field, click a radio button to select IPv4 or IPv6.
7. In the **SecondaryServerInetAddress** field, type the secondary IP address.
8. In the **State** field, click a radio button.
9. In the **SyncInterval** field, type a value.
10. In the **ManualSyncRequest** field, click the radio button to synchronize the switch clock with the NTP server.
11. On the toolbar, click **Apply**.

Variable definitions

The following table describes configuring SNTP.

Variable	Value
PrimaryServerInetAddressType	Specifies the IP address type of the primary SNTP server. Values include IPv4 or IPv6.
PrimaryServerInetAddress	Specifies the IP address of the primary SNTP server.

Variable	Value
SecondaryServerInetAddressType	Specifies the IP address type for the secondary SNTP server. Values include IPv4 or IPv6.
SecondaryServerInetAddress	Specifies the IP address of the secondary SNTP server.
State	Specifies if SNTP is used to synchronize the switch clock to the Coordinated Universal Time (UTC) • disabled — the switch cannot synchronize the clock using SNTP. • enabled (unicast) — the switch synchronizes to UTC on boot when network access is available, and periodically synchronizes based on the Sync Interval.
SynchInterval	Specifies the frequency, in hours, to attempt synchronization with the NTP servers. Values range from 0 to 168. 0 indicates to synchronize only during boot.
ManualSyncRequest	Specifies to immediately attempt a synchronization with the NTP servers.
LastSyncTime	Indicates the last synchronization time in UTC.
LastSyncSourceInetAddressType	Indicates the IP source address type of the NTP server during the last synchronization.
LastSyncSourceInetAddress	Indicates the IP source address of the NTP server during the last synchronization.
NextSyncTime	Indicates the next scheduled synchronization time in UTC.
PrimaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the primary server address. Synchronization with the secondary server can still occur.
SecondaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the secondary server address.
CurrentTime	Indicates the current switch time in UTC.

Configuring the local time zone

Use the following procedure to configure the local time zone.

Procedure

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

Variable definitions

The following table describes configuring the local time zone

Variable	Value
TimeZone	Specifies the local time zone of the switch, measured as an offset in 15 minute increments from Greenwich Mean Time (GMT).
TimeZoneAcronym	Specifies the time zone acronym to display.

Configuring daylight savings time

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

Before you begin

Recurring daylight savings time must be disabled.

Procedure

1. From the navigation tree, double-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** field, type a value.
5. In the **TimeZoneAcronym** field, type a value.
6. In the **StartYear** field, type a value.
7. In the **StartMonth** field, type a value.
8. In the **StartDay** field, type a value.
9. In the **StartHour** field, type a value.
10. In the **StartMinutes** field, type a value.
11. In the **EndYear** field, type a value.
12. In the **EndMonth** field, type a value.
13. In the **EndDay** field, type a value.
14. In the **EndHour** field, type a value.
15. In the **EndMinutes** field, type a value.
16. To enable daylight savings time, click the **Enabled** check box. To disable daylight savings time, clear the check box.
17. Click **Apply**.

Variable definitions

The following table describes configuring daylight savings time.

Variable	Value
Offset	Specifies the change of time in minutes when daylight savings time (DST) starts and ends. The offset is added when DST starts and is subtracted when DST time ends.
TimeZoneAcronym	Specifies the time zone acronym to display.
StartYear	Specifies the year to start DST.
StartMonth	Specifies the month to start DST.
StartDay	Specifies the day to start DST.
StartHour	Specifies the hour to start DST.
StartMinutes	Specifies minutes in the specific hour to start DST.

Variable	Value
EndYear	Specifies the year to end DST.
EndMonth	Specifies the month to end DST.
EndDay	Specifies the day to end DST.
EndHour	Specifies the hour to end DST.
EndMinutes	Specifies the minutes in the specific hour to end DST.
Enabled	Specifies if DST is enabled or disabled. Check to enable, clear to disable. **Important:** Configure all DST fields before you enable DST.

Configuring recurring daylight savings time

Use the following procedure to configure recurring daylight savings time start and end times.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **SNTP/Clock**.
3. In the work area, click the **Summer Time Recurring** tab
4. To enable recurring daylight savings time, click the **Recurring** check box. To disable recurring daylight savings time, clear the check box.
5. In the **RecurringStartMonth** field, select a month from the list.
6. In the **RecurringStartWeek** field, click a radio button.
7. In the **RecurringStartDay** field, select a day from the list.
8. In the **RecurringStartHour** field, select an hour from the list.
9. In the **RecurringStartMinute** field, type a value.
10. In the **RecurringEndMonth**, select a month from the list.
11. In the **RecurringEndWeek**, click a radio button.
12. In the **RecurringEndDay** field, select a day from the list.
13. In the **RecurringEndHour** field, select an hour from the list.
14. In the **RecurringEndMinute** field, type a value.

15. In the **RecurringOffset** field, type a value.
16. On the toolbar, click **Apply**.

Variable definitions

The following table describes configuring recurring daylight savings time.

Variable	Value
Recurring	Specifies to enable or disable recurring daylight savings time. Click to enable, clear to disable.
RecurringStartMonth	Specifies the month of each year to start DST.
RecurringStartWeek	Specifies the week of the month to start DST. If week 5 is selected and not available in a certain year, recurring start uses the 'last' option. For example, in a year without a Sunday in the fifth week of March, DST starts on the last Sunday of March.
RecurringStartDay	Specifies the day to start DST.
RecurringStartHour	Specifies the hour to start DST.
RecurringStartMinutes	Specifies minutes in the specific hour to start DST.
RecurringEndMonth	Specifies the month to end DST.
RecurringEndWeek	Specifies the week of the month to end DST. If week 5 is selected and not available in a certain year, recurring end uses the 'last' option. For example, in a year without a Sunday in the fifth week of October, DST ends on the last Sunday of October.
RecurringEndDay	Specifies the day to end DST.
RecurringEndHour	Specifies the hour to end DST.
RecurringEndMinutes	Specifies the minutes in the specific hour to end DST.
RecurringOffset	Specifies the time in minutes to change the time when DST starts and ends. The offset is added to the current time when DST starts, and is subtracted when DST ends.

Avaya Energy Saver configuration

You can use Avaya Energy Saver (AES) to configure the switch to utilize energy more efficiently.

Configuring global AES

Use this procedure to configure AES for a single switch or a stack

Procedure

1. From the navigation tree, double-click **Power Management**
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select (to enable) or deselect (to disable) AES parameters as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

Variable Definitions

The following table outlines the parameters of the **Energy Saver Globals** tab.

Variable	Value
EnergySaverEnabled	Enables or disables energy saving for the switch.
PoePowerSavingEnabled	Enables or disables AES PoE power save mode for the switch. When enabled, AES PoE power saver mode provides the capability to control power consumption savings for only orts that have AES enabled, and PoE priority configured to low.
EfficiencyModeEnabled	Enables or disables AES efficiency mode for the switch. When enables, AES efficeincy mode enables AES globally and for each port, enables AES PoE power save mode, and configures AES scheduling to

Variable	Value
	predetermined values (on time 18:00 and off time 07:30 daily). **Important:** AES efficeincy mode overrides custom AES scheduling and PoE power saving mode. You will be prompted to confirm that you want to enable AES efficiency mode before proceeding.
EnergySaverActive	Activates or deactivates the Avaya Energy Saver.

Configuring the AES schedule

Use this procedure to configure the start or end of a time interval for the switch to enter lower power states. The time interval can span a complete week, a complete weekend, multiple days, or be configured within an individual day.

Before you begin

- Disable AES globally

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Schedules** tab.
4. Click **Insert**.
5. To choose a day for the AES schedule on time, click a button in the **ScheduleDay** section.
6. To choose an hour of the day for the AES schedule on time, type a value in the **ScheduleHour** box.
7. To choose a portion of an hour for the AES schedule on time, type a value in the **ScheduleMinute** box.
8. To configure the selected day, hour, and minutes as the AES schedule on time, click the **activate** button in the **ScheduleAction** section.

   Activate is selected by default.
9. To configure the selected day, hour, and minutes as the AES schedule off time, click the **deactivate** button in the **ScheduleAction** section.

10. Click **Insert**.

Variable Definitions

The following table describes the fields of **Insert Energy Saver Schedule** window.

Variable	Value
ScheduleDay	Indicates the day on which this schedule entry takes effect.
ScheduleHour	Indicates the hour on which this schedule entry takes effect.
ScheduleMinute	Indicates the Minute on which this schedule entry takes effect.
ScheduleAction	Activates or deactivates the energy savings.

Modifying an AES schedule on and off time status

Use this procedure to change an existing schedule off time to on time or to change an existing schedule on time to off time.

Before you begin

• Disable AES globally

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Schedules** tab.
4. To select a schedule time to edit, click a schedule day.
5. In the schedule day rowdouble-click the cell in the **ScheduleAction** column.
6. Select a value from the list—**activate** to configure the schedule time as the on time, or **deactivate** to configure the schedule time as the off time.
7. Click **Apply**.

Configuring port-based AES

Use this procedure to configure port-based AES to enable or disable energy saving for individual ports, or all ports on a switch or stack.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Ports** tab.
4. In the **Multiple Port Configuration** area, click the **Switch/Stack/Ports** elipsis **(...)**.
5. Click a port or ports, or click **All**.
6. Click **Ok**.
   The portlist appears in the **Switch/Stack/Ports** box.
7. In the **Multiple Port Configuration** area double-click the cell under **EnergySaverEnabled**.
   Select **true** to enable AES or **false** to disable AES for the port(s).
8. Click **Apply Selection**.
9. On the toolbar, click **Apply**.
10. Repeat steps 4 to 9 to enable AES for additional ports as required.
11. Click **Apply**.
12. On the toolbar, you can click **Refresh** to update the work area data display.

Variable definitions

The following table outlines the parameters of the **Ports** tab.

Variable	Value
Port	Indicates the port.
EnergySaverEnabled	Indicates whether the Avaya Energy Saver feature is enabled for the port.
EnergySaverPoeStatus	Indicates the Energy Saver PoE status. Values include:

Variable	Value
	• notApplicable • enabled • disabled

Viewing AES information

Use this procedure to display energy saving information for an individual switch or switches in a stack.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Savings** tab.
4. On the toolbar, you can click **Refresh** update the data.

Variable definitions

The following table outlines the parameters of the **Energy Savings** tab.

Variable	Value
UnitIndex	Indicates the unit number of the switch.
UnitSavings(watts)	Indicates the total power capacity being saved on the switch.
PoeSavings(watts)	Indicates the total PoE power being saved on the switch.

Chapter 15: Configuring and testing ports using EDM

Use the procedures in this section to configure port features such as the port speed, duplex operation, and autotopology using Enterprise Device Manager (EDM).

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. In the port row, double-click the cell in the **FlowControlAdminMode** column and select a value from the list.
13. In the port row, double-click the cell in the **AutoNegotiationAdvertisements** column and select one or more values from the list.
14. Repeat steps 5 through 11 to configure additional interface ports.
15. On the toolbar, click **Apply**.
16. 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 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

Variable	Value
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 • enabledRcv - receive enabled • enabledXmitAndRcv - transmit and receive enabled
FlowControlOperMode	Indicates the current flow control mode of the port.
AutoNegotiationCapability	Specifies the prot speed and duplex capabilities that a switch can support on a port, and that can be advertised by the port using auto-negotiation.
AutoNegotiationAdvertisements	Specifies the port speed and duplex abilities to be advertised during link negotiation. Values include:

Variable	Value
	• 10Half • 10Full • 100Half • 100Full • 1000Full • PauseFrame • AsymmPauseFrame
WanMode	Values include: • none • wan • lan
MItd	Indicates the MultiLink Trunk assigned to the port.
IsPortShared	Specifies whether a port is shared. Multiple ports that are logically represented as a single port are shared. Only one shared port can be active at a time.
PortActiveComponent	Indicates the port components active for a shared port.

Configuring Rate Limiting

Use the following procedure to configure Rate Limiting on interface ports.

Before you begin

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

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 **Rate Limit** tab.
5. To select an interface port to rate limit, click a port row the **Index** column.

6. In the port row, double-click the cell in the **AllowedRate** column and select a value from the list.
7. In the port row, double-click the cell in the **AllowedRatePps** column and select a value from the list.
8. In the port row, double-click the cell in the **Enable** column and select a value from the list.
9. On the toolbar, click **Apply**.

Variable definitions

The following table describes configuring Rate Limiting

Variable	Value
Index	Indicates the unique identifier for a port.
TrafficType	Indicates the type of traffic to configure with rate limiting. Values include broadcast and multicast.
AllowedRate	Specifies the rate limiting percentage. Values range from 0 percent (none) to 10 percent..
AllowedRatePps	Values range from 0 to 262143
Enable	Specifies if rate limiting is enabled or disabled. Values include true (enabled) or false (disabled).

Testing port cables

Use this procedure to initiate a TDR test.

About this task

The 5000 Series switch is equipped with a Time Domain Reflectometer (TDR). The TDR provides a diagnostic capability to test connected cables for defects (such as short pin and pin open). Use the TDR tab to initiate cable diagnostic tests on attached cables.

The cable diagnostic tests only apply to Ethernet copper ports; fiber ports cannot be tested. You can initiate a test on multiple ports at the same time.

When you test a cable with the TDR, if the cable has a 10/100 MB/s link, the link is broken during the test and restored only when the test is complete. Use of the TDR does not affect 1 GB/s links.

Note:

The accuracy margin of cable length diagnosis is between three to five meters. Avaya suggests the shortest cable for length information be five meters long.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Ports**.
4. In the work area, click the **TDR** tab.
5. Select the **StartTest** option.
6. Click **Apply**.

TDR field descriptions

The following table outlines the parameters for the **TDR** tab.

Name	Description
StartTest	Enables the TDR test.
TestDone	Indicates whether a TDR test is complete.
CableStatus	Indicates the status of the cable as a whole. The status of a cable is, in a sense, a summation of the status of its pairs. If all the pairs are normal, the cable is normal. If the cable consists of zero or more normal pairs and one or more open pairs, the cable is considered open. If the cable consists of shorted pairs and normal pairs, it is considered shorted. Any combination of open and shorted pairs is considered simply failed. • **cableFail** • **cableNormal** • **cableOpen** • **cableShorted**

Name	Description
	• **cableNotApplicable** • **cableUntested**
Pair1Status	The status of a single pair in the cable: • **pairFail** • **pairNormal** • **pairOpen** • **pairShorted** • **pairNotApplicable** • **pairNotTested** • **pairForce** **Note:** If a 10MB or 100MB link is established without autonegotiation, Pair 1 will return Forced mode. The pair length is meaningless in this case.
Pair1Length	Pair Length, in meters, measured by Time Domain Reflectometry.
Pair2Status	The status of a single pair in the cable.
Pair2Length	Pair Length, in meters, measured by Time Domain Reflectometry.
Pair3Status	The status of a single pair in the cable.
Pair3Length	Pair Length, in meters, measured by Time Domain Reflectometry.
Pair4Status	The status of a single pair in the cable.
Pair4Length	Pair Length, in meters, measured by Time Domain Reflectometry.
CableLength	Length of cable in meters based on average electrical length of 4 pairs. Measurement can be done when traffic is live or not.
Pair1Polarity	The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair1Swap	The pair swap in the cable: • **normal** • **swapped**

Name	Description
	• **invalid** • **error** This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair1Skew	Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.
Pair2Polarity	The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair2Swap	The pair swap in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair2Skew	Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.
Pair3Polarity	The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair3Swap	The pair swap in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.
Pair3Skew	Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.
Pair4Polarity	The polarity of a single pair in the cable.
Pair4Swap	The pair swap in the cable.
Pair4Skew	Differential cable pair length in meters. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.

Chapter 16: Updating switch software using EDM

Use the procedures in this section to update the switch software, which is a necessary part of switch configuration and maintenance.

Before you begin

- The switch must be assigned a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is present on the network that is accessible by the switch and that has the desired software version loaded.
- If you change the switch software with software stored on a USB mass storage device, ensure that the mass storage device has the desired software version loaded on it and is inserted into the front panel USB port.

About this task

The ERS 5600 Series supports the Dual Agent feature. This feature provides two agent images: the Agent Primary image and the Agent Secondary image. The Agent Primary image represents the agent image used for the next boot. You can select either image for the next boot. The Dual Agent Boot flag determines which agent image is the boot image. The diagnostics and agent software must use the same value for the Dual Agent Boot flag. If the Dual Agent Boot flag is not set, the unit will boot from Agent 1 (default).

During the software download process, the port LEDs light one after another in a chasing pattern. This chasing pattern is initially fast as the software image is downloaded but gradually slows as the switch erases the flash memory. This pattern speeds up again as the switch programs the new image into the flash memory. When the process is complete, the port LEDs are no longer lit and the switch resets.

Displaying boot image and flash information

Use the following procedure to display the currently loaded and operational agent, image, and flash load status for the switch or stack.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. In the work area, click the **FLASH** tab.

Variable definitions

The following table describes displaying boot images.

Variable	Value
Unit	Specifies the unit.
Type	Specifies the type of image.
Version	Specifies the software version of the image.
Description	Specifies a description of the image.
Age	Specifies the age.

Managing the configuration and image files

Use the following procedure to upgrade, save, or restore a binary configuration, image, or diagnostic file.

About this task

You can use the Config/Image/Diag file tab to transfer binary files to or from a TFTP server or a USB storage device. You can upgrade the switch agent image or diagnostic image.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. In the work area, click the **Config/Image/Diag file** tab.
4. To transfer files using a TFTP server, In the **TFTPServerInetAddressType** field, click a radio button.
5. To transfer files using a TFTP server, In the **TFTPServerInetAddress** field, type an IP address.
6. To transfer a configuration file, in the **BinaryConfigFilename** field, type a filename.
7. To transfer a configuration file, in the **BinaryConfigUnitNumber** field, enter a value.
8. To transfer an agent image file, in the **ImageFileName** field, type a filename.
9. To transfer a diagnostic image file, in the **FWFileName(Diagnostics)** field, type a filename.

10. In the **Usb TargetUnit** field, type a value.

    Important:

    You must enter a value in the Usb TargetUnit field. Type 1 to 8 for a unit, 9 for a standalone unit, 0 for TFTP server, or 10 for SFTP server.

11. To download an agent image file as primary or secondary, in the **Image** field, click a radio button.
12. In the **Action** field, click a radio button.
13. On the toolbar, click **Apply**.
14. In the **Status** field, view and verify the status of your action.

Result

The transfer process occurs immediately after clicking Apply. You can only perform one action at a time.

Important:

If you are downloading an agent image, the process erases the contents of flash memory and replaces it with the new image. Do not interrupt the download process. Depending on network conditions, the process can take up to 10 minutes.

EDM provides a status bar on the progress of your software download. If you are downloading without using a NoReset option, EDM displays the estimated time for rebooting the switch. Otherwise, when the download process is complete, a message appears with an option to reboot the switch immediately . The switch can automatically reset and the new software image initiates a self test. During the agent image download process, the switch is not operational.

Variable definitions

The following table describes managing binary configuration, image, and diagnostic files.

Variable	Value
TftpServerInetAddressType	Specifies the IP address type of the TFTP or SFTP server. Values include IPv4 or IPv6.
TftpServerInetAddress	Specifies the IP address of the TFTP or SFTP server.
BinaryConfigFilename	Specifies the binary configuration file currently associated with the switch. This field only applies to binary configuration files.

Variable	Value
BinaryConfigUnitNumber	Specifies the unit number portion of the configuration file to be used for the standalone unit configuration. Values range from 0 to 8. If 0, the unit number is ignored. This field only applies to binary configuration files.
ImageFileName	Specifies the name of the image file currently associated with the switch. You can change this field to the filename 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 filename of the software image to be downloaded.
Usb TargetUnit	Specifies the unit number for USB, or the transfer type to use during the upload or download operation. Values include: • 1 to 8 — USB on unit 1 to 8 • 9 — USB on a standalone unit • 0 — TFTP server • 10 — SFTP server
Image	Specifies if the image to download is the primary or secondary image.
Action	Specifies the action to perform during the file transfer. Values include: • other — no action • dnldConfig — Downloads the configuration file from a TFTP or SFTP server • upldConfig — Uploads the configuration file to a TFTP or SFTP server • dnldConfigFromUsb — Downloads the configuration file from a USB storage device. • upldConfigToUsb — Uploads the configuration file to a USB storage device. • dnldImg — Downloads the agent image file from a TFTP or SFTP server. • dnldImgIfNewer — Only downloads if newer than current image.

Variable	Value
	• dnldImgNoReset — Downloads the agent image and does not reset the switch. • dnldImgFromUsb — Downloads the agent image from a USB storage device. • dnldFw — Downloads the diagnostic image from a TFTP server. • dnldFwNoReset — Downloads the diagnostic image and does not reset the switch. • dnldFwFromUsb — Downloads the diagnostic image from a USB storage device.
Status	Indicates the status of the last action since the last switch reboot. Values include: • other — No action has taken place. • inProgress — The selected action is currently in process. • success — The selected action completed successfully. • fail — The selected action failed.

Chapter 17: Configuring a Virtual Fabric using EDM

Use the procedures in this section to configure a Virtual Fabric (stack) using Enterprise Device Manager (EDM).

Configuring Auto Unit Replacement

Use the following procedure to configure Auto Unit Replacement (AUR).

Procedure

1. From 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 **AUR** tab.
5. To enable AUR, select the **AutoUnitReplacementEnable** check box. To disable AUR, clear the check box.
6. To enable AUR configuration saves, select the **AutoUnitReplacementSaveEnabled** check box. To disable AUR saves, clear the check box.
7. In the **AutoUnitReplacementForceSave** field, type a value.
8. In the **AutoUnitReplacmentRestore** field, type a value.
9. On the toolbar, click **Apply**.

Variable definitions

The following table describes configuring Auto Unit Replacement.

Variable	Value
AutoUnitReplacementEnabled	Specifies if AUR is enabled or disabled. Check to enable, clear to disable.

Variable	Value
AutoUnitReplacementSaveEnabled	Specifies if AUR automatic saves of unit configuration images is enabled or disabled. Check to enable, clear to disable.
AutoUnitReplacementForceSave	Specifies to manually save a specific non-base unit configuration image to the base unit. Value range of 0 to 8.
AutoUnitReplacementRestore	Specifies to manually restore the configuration of a specific non-base unit from the saved configuration image on the base-unit. Value range of 0 to 8.

Configuring the base unit

Use the following procedure to configure the base unit. and to display base unit information.

About this task

You can use the Base Unit Info tab to reset the base unit, to enter a location for the base unit, or to view base unit status information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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** field, click a radio button.
6. In the **Location** field, type a character string.
7. On the toolbar, click **Apply**.

Variable definitions

The following table describes configuring and displaying the base unit status.

Variable	Value
Type	Indicates the switch type.
Descr	Indicates the switch port description.

Variable	Value
Ver	Indicates the switch hardware version.
SerNum	Indicates the switch serial number.
LstChng	Indicates the sysUpTime when the interface entered the 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 include enable or reset. **Important:** In a stack configuration, the reset option resets only the base unit.
OperState	Indicates the operational state of the switch.
Location	Specifies the physical location of the switch.
RelPos	Indicates the relative position of the switch.
BaseNumPorts	Indicates the number of base ports on 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.

Configuring stack units

Use the following procedure to configure stack units, and to display stack unit information.

About this task

You can use the Stack Info tab to reset stack units, to enter a location for stack units, or to view stack unit status information.

Procedure

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

3. In the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Stack Info** tab.
5. In a unit row, double-click the **Location** cell and type a character string.
6. In a unit row, double-click the **AdminState** cell and select a value from the list.
7. On the toolbar, click **Apply**.

Variable definitions

The following table describes configuring and displaying the stack unit status.

Variable	Value
Indx	Indicates the unique identifier number for the stack unit.
Descr	Indicates the stack unit port description.
Location	Specifies the physical location of the stack unit.
LstChng	Indicates the sysUpTime when the interface entered the 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 stack unit. Values include enable or reset.
OperState	Indicates the operational state of the stack unit.
Ver	Indicates the stack unit hardware version.
SerNum	Indicates the stack unit serial number.
BaseNumPorts	Indicates the number of base ports on the stack unit.
TotalNumPorts	Indicates the total number of ports on the stack unit.
IpAddress	Indicates the stack unit IP address.
RunningSoftwareVer	Indicates the version of the running software.

Renumbering stack units

Use the following procedure to change the unit number of switches in a stack.

Before you begin

A stack configuration is required to change unit numbers in a stack.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Stack Numbering** tab.
5. To select a switch unit, click a unit row.
6. In the unit row, double-click the cell in the **New Unit Number** column and select a number from the list.
7. On the toolbar, click **Apply**.

Result

A warning message appears indicating that renumbering a unit results in an automatic reset of the stack.

Variable definitions

The following table describes renumbering a unit in a stack.

Variable	Value
Current Unit Number	Indicates the current unit number of the switch.
Descr	Indicates the port description of the switch.
New Unit Number	Specifies a new unit number for the switch. The stack automatically resets if you change the unit number.

Viewing stack mode properties

Use this procedure to view the stack mode properties of the switch.

Procedure

1. From 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 **Stack Mode** tab.

Stack Mode field descriptions

The following table outlines the parameters of the **Stack Mode** tab.

Name	Description
CurrentOperationMode	Specifies the operational mode.
NextBootOperationMode	Specifies the boot operation mode.

Chapter 18: Managing Power over Ethernet (PoE) using EDM

Managing switch PoE

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

Procedure

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

     OR

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

PoE tab field descriptions

The following table outlines the parameters of the **PoE** tab.

Name	Description
Power(watts)	Displays the total power (in watts) available to the switch.
OperStatus	Displays the power state of the switch: • **on** • **off** • **faulty**
ConsumptionPower(watts)	Displays the power (in watts) being used by the switch.
UsageThreshold%	Lets you set a percentage of the total power usage of the switch above which the system sends a trap. **Important:** You must enable the traps (NotificationControlEnable) to receive a power usage trap.
NotificationControlEnable	Lets you enable or disable sending traps if the switch power usage exceeds the percentage set in the UsageThreshold% field.
PoweredDeviceDetectType	Lets you set the power detection type that the switch uses to detect a request for power from a device connected to all ports on the switch: • **802.3af** • **802.3af and legacy support**
PowerPairs	A read-only field that displays the status of the RJ-45 pin pairs that the switch uses to send power to the ports on the switch.

Viewing PoE information for switch ports

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

Procedure

1. From the **Device Physical View**, select a port.
2. In the navigation tree, click **Edit**.
3. In the Edit tree, click **Chassis**.
4. Click **Ports**.
5. In the work area, click the **PoE** tab.

PoE tab field descriptions

The following table describes the fields on the PoE tab.

Name	Description
AdminEnable	Lets you enable or disable PoE on this port. By default, PoE is enabled.
PowerPairs	Displays the status of the RJ-45 pin pairs that the switch uses to send power to the prots on the switch.
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**

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

Appendix A: Factory default configuration

Factory default configuration settings

Setting	Factory Default Configuration Value
Unit Select switch	non-Base
Unit	1
BootP Request Mode	Disabled
In-Band Stack IP Address	192.168.1.2
In-Band Switch IP Address	192.168.1.1
In-Band Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0 (no IP address assigned)
Read-Only Community String	public
Read-Write Community String	private
Trap IP Address	0.0.0.0 (no IP address assigned)
Community String	Zero-length string
Authentication Trap	Enabled
Autotopology	Enabled
sysContact	Zero-length string
sysName	Zero-length string
sysLocation	Zero-length string
Aging Time	300 seconds
Find an Address	00-00-00-00-00-00 (no MAC address assigned)
Select VLAN ID [1]	
MAC Address Security	Disabled
MAC Address Security SNMPLocked	Disabled
Partition Port on Intrusion Detected	Disabled
Partition Time	0 seconds (the value 0 indicates forever)
DA Filtering on Intrusion Detected	Disabled
Generate SNMP Trap on Intrusion	Disabled

Setting	Factory Default Configuration Value
Clear by Ports	NONE
Learn by Ports	NONE
Current Learning Mode	Not Learning
Trunk	blank field
Security	Disabled
Port List	blank field
Find an Address	blank field
MAC Address	00-00 00-00 -00-00
Allowed Source	blank field
Display/Create MAC Address	00-00-00-00-00-00
Create VLAN	1
Delete VLAN	blank field
VLAN Name	VLAN #
Management VLAN	Yes (VLAN #1)
VLAN Type	Port-based
Protocol ID (PID)	None
User-Defined PID	0x0000
VLAN State	Active (VLAN # 1)
Port Membership	All ports assigned as members of VLAN 1
Unit	1
Port	1
Filter Untagged Frames	No
Filter Unregistered Frames	Yes
Port Name	Unit 1, Port 1
PVID	1
Port Priority	0
Tagging	Untag All
AutoPVID	Enabled
Unit	1
Port	1
PVID	1 (read only)

Setting	Factory Default Configuration Value
Port Name	Unit 1, Port 1 (read only)
Unit	1
Linktrap	On
Autonegotiation	Enabled (for all ports)
Speed/Duplex	(See Autonegotiation)
Trunk	1 to 32 (depending on configuration status)
Trunk Members (Unit/Port)	Blank field
STP Learning	Normal
Trunk Mode	Basic
Trunk Status	Disabled
Trunk Name	Trunk #1 to Trunk #32
Traffic Type	Rx and Tx
Port	1
Monitoring Mode	Disabled
Monitor/Unit Port	Zero-length string
Unit/Port X	Zero-length string
Unit/Port Y	Zero-length string
Address A	00–00–00–00–00–00 (no MAC address assigned)
Address B	00–00–00–00–00–00 (no MAC address assigned)
Rate Limit Packet Type	Both
Limit	None
VLAN	1
Snooping	Disabled
Proxy	Disabled
Robust Value	2
Query Time	125 seconds
Static Router Ports	- (for all ports)
Multicast Group Membership screen	
Unit	1
Port	1
Console Port Speed	9600 Baud

Setting	Factory Default Configuration Value
Console Switch Password type	None
Console Stack Password type	None
Telnet Stack Password type	None
Telnet Switch Password type	None
Console Read-Only Switch Password	Passwords are user for non-SSH software images and userpasswd for SSH software images.
Console Read-Write Switch Password	Passwords are secure for non-SSH software images and securepasswd for SSH software images.
Console Read-Only Stack Password	Passwords are user for non-SSH software images and userpasswd for SSH software images.
Console Read-Write Stack Password	Passwords are secure for non-SSH software images and securepasswd for SSH software images.
Radius password/server	secret
New Unit Number	Current stack order
Renumber units with new setting?	No
Group	1
Bridge Priority	8000
Bridge Hello Time	2 seconds
Bridge Maximum Age Time	20 seconds
Bridge Forward Delay	15 seconds
Add VLAN Membership	1
Tagged BPDU on tagged port	• STP Group 1--No • Other STP Groups--Yes
STP Group State	• STP Group 1--Active • Other STP Groups--InActive
VID used for tagged BPDU	4001-4008 for STGs 1-8, respectively
STP Group	1
Participation	Normal Learning
Priority	128
Path Cost	1
STP Group	1

Setting	Factory Default Configuration Value
STP Group	1
TELNET Access/SNMP	By default, SNMP access is disabled in the SSH image and enabled in the non-SSH image. Telnet is enabled by default in both SSH and non-SSH images. Use list: Yes
Login Timeout	1 minute
Login Retries	3
Inactivity Timeout	15 minutes
Event Logging	All
Allowed Source IP Address (50 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)
	Remaining 49 fields: 255.255.255.255 (any address is allowed)
Allowed Source Mask (50 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)
	Remaining 49 fields: 255.255.255.255 (any address is allowed)
	Remaining 49 fields: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 (any IPv6 address is allowed)
Image Filename	Zero-length string
Diagnostics image filename	Zero-length string
TFTP Server IP Address	0.0.0.0 (no IP address assigned)
Start TFTP Load of New Image	No
Configuration Image Filename	Zero-length string
Copy Configuration Image to Server	No
Retrieve Configuration Image from Server	No
ASCII Configuration Filename	Zero-length string
Retrieve Configuration file from Server	No
Auto Configuration on Reset	Disabled
High Speed Flow Control Configuration	
VLAN Configuration Control	Strict
Agent Auto Unit Replacement	Enabled

Glossary

ACLI modes	Differing command modes are available within the text-based interface, dependant on the level of user permissions determined by logon password. Each successive mode level provides access to more complex command sets, from the most restrictive—show level only, to the highest configuration levels for routing parameters, interface configuration, and security.
Auto Unit Replacement (AUR)	Allows users to replace a unit from a stack while retaining the configuration of the unit. Stack power must remain on during the unit replacement. AUR does not work in a stack of two units only.
Auto-Detection and Auto-Configuration (ADAC)	Provides automatic switch configuration for IP phone traffic support and prioritization. ADAC can configure the switch whether it is directly connected to the Call Server or uses a network uplink.
Autonegotiation	Allows the switch to select the best speed and duplex modes for communication between two IEEE-capable devices.
Autosensing	Determines the speed of the attached device if it is incapable of autonegotiation or if it uses an incompatible form of autonegotiation. The switch reverts to half-duplex mode if the duplex mode of the attached device cannot be determined.
Autotopology	An Enterprise Network Management System (ENMS) protocol that automates and simplifies discovery and collection of network topology information, presented in a table.
Avaya command line interface (ACLI)	A textual user interface. When you use ACLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.
Border Gateway Protocol (BGP)	An inter-domain routing protocol that provides loop-free inter-domain routing between Autonomous Systems (AS) or within an AS.
Domain Name System (DNS)	A system that maps and converts domain and host names to IP addresses.
Dynamic Host Configuration Protocol (DHCP)	A standard Internet protocol that dynamically configures hosts on an Internet Protocol (IP) network for either IPv4 or IPv6. DHCP extends the Bootstrap Protocol (BOOTP).

Enterprise Device Manager (EDM)	A Web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.
Internet Group Management Protocol (IGMP)	IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.
Link Aggregation Control Protocol (LACP)	A network handshaking protocol that provides a means to aggregate multiple links between appropriately configured devices.
Link Layer Discovery Protocol (LLDP)	Link Layer Discovery Protocol is used by network devices to advertise their identities. Devices send LLDP information at fixed intervals in the form of Ethernet frames, with each frame having one Link Layer Discovery Protocol Data Unit.
Open Shortest Path First (OSPF)	A link-state routing protocol used as an Interior Gateway Protocol (IGP).
out of band (OOB)	Network dedicated for management access to chassis.
Power over Ethernet (PoE)	The capacity of a switch to power network devices, according to the 802.3af standard, over an Ethernet cable. Devices include IP phones, Wireless LAN Access Points (WLAN AP), security cameras, and access control points.
rate limiting	Rate limiting sets the percentage of traffic that is multicast, broadcast, or both, on specified ports.
Routing Information Protocol (RIP)	A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. You often use RIP as a very simple interior gateway protocol (IGP) within small networks.
Secure Shell (SSH)	SSH uses encryption to provide security for remote logons and data transfer over the Internet.
Secure Sockets Layer (SSL)	An Internet security encryption and authentication protocol for secure point-to-point connections over the Internet and intranets, especially between clients and servers.
Simple Network Time Protocol (SNTP)	Provides a simple mechanism for time synchronization of the switch to any RFC 2030-compliant Network Time Protocol (NTP) or SNTP server.
stack IP address	An IP address must be assigned to a stack so that all units can operate as a single entity.

Time Domain Reflectometer (TDR)	Provides diagnostic capability on Ethernet copper ports to test connected cables for defects. The TDR interrupts 10/100 MB/s links but does not affect 1 GB/s links.
Virtual Local Area Network (VLAN)	A Virtual Local Area Network is a group of hosts that communicate as if they are attached to the same broadcast domain regardless of their physical location. VLANs are layer 2 constructs.
virtual router forwarding (VRF)	Provides traffic isolation between customers operating over the same node. Each virtual router emulates the behavior of a dedicated hardware router by providing separate routing functionality, and the network treats each VRF as a separate physical router.
Virtual Router Redundancy Protocol (VRRP)	A protocol used in static routing configurations, typically at the edge of the network. This protocol operates on multiple routers on an IP subnet and elects a primary gateway router. When the primary router fails, a backup router is quickly available to take its place.