Configuration — System
Avaya Ethernet Routing Switch 4500 Series

5.5
NN47205-500, 07.01
April 2011

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

Copyright

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: New in this release

The following sections detail what is new in *Avaya Ethernet Routing Switch 4500 Configuration — System* (NN47205-500) for Release 5.5.

Features

See the following sections for information about feature changes:

802.1AB customization

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

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

- System TLV
- Port Description TLV
- System Name TLV
- System Description TLV
- System Capability TLV
- Management Address TLV
- VLAN Name TLV
- Port VLAN ID TLV
- Port and Protocol VLAN ID TLV
- MAC/PHY configuration/status TLV
- Power via MDI TLV, Link Aggregation TLV
- Maximum Frame Size TLV
- LLDP MED Capabilities TLV
- Network Policy TLV

- Location Identification TLV
- Extended Power-via-MDI TLV and Inventory TLV

You can also configure the following timers:

- Reinitialisation Delay
- Transmit Interval
- Transmit Delay
- Transmit Hold
- Fast Start Timers
- LLDP Timers
- SNMP Notification Interval

802.1AB integration

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

New 802.1AB default parameters

Beginning with Release 5.5, you can improve Voice and Video over IP function because some of the LLDP parameters are enabled by default. Now you can connect LLDP enabled IP handsets to the switch and start deployment without additional configuration. The following LLDP parameters are enabled by default:

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

Chapter 2: Introduction

This document provides the information and procedures required to configure the software for the Avaya Ethernet Routing Switch 4500 Series.

Unless otherwise indicated, this information applies to

- Avaya Ethernet Routing Switch 4524GT
- Avaya Ethernet Routing Switch 4524GT-PWR
- Avaya Ethernet Routing Switch 4526FX
- Avaya Ethernet Routing Switch 4526GTX
- Avaya Ethernet Routing Switch 4526GTX -PWR
- Avaya Ethernet Routing Switch 4526T
- Avaya Ethernet Routing Switch 4526T-PWR
- Avaya Ethernet Routing Switch 4550T
- Avaya Ethernet Routing Switch 4550T-PWR
- Avaya Ethernet Routing Switch 4548GT
- Avaya Ethernet Routing Switch 4548GT-PWR

The term "Avaya Ethernet Routing Switch 4500 Series" is used in this document to describe the features common to the switches mentioned in the preceding list.

A switch is referred to by its specific name while describing a feature exclusive to the switch.

The Avaya Ethernet Routing Switch 4500 Series switches operate in the Standalone Mode and Stacking Mode in this product release. A switch can be in Standalone Mode or in Stacking Mode, not both.

ACLI command modes

ACLI provides the following command modes:

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

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

Table 1: ACLI command modes

Command mode and sample prompt	Entrance commands	Exit commands

User EXEC
`4548GT-PWR>`
	No entrance command, default mode	`exit`
		or
		`logout`

Privileged EXEC
`4548GT-PWR#`
	`enable`	`exit`
		or
		`logout`

Global Configuration
`4548GT-PWR(config)#`
	`configure terminal`	mode, enter:
		`end`
		or
		`exit`
		To exit ACLI completely, enter:
		`logout`

Interface Configuration
`4548GT-PWR(config-if)#`
interface vlan
	From Global Configuration mode: To configure a port, enter:
	`interface fastethernet`
	<port number> To configure a VLAN, enter: interface vlan <vlan number>
		To return to Global Configuration mode, enter:
		`Exit`
		To return to Privileged EXEC mode, enter:
		`end`
		To exit ACLI completely, enter:
		`logout`

For more information, see *Avaya Ethernet Routing Switch 4500 Series Fundamentals* (NN47205-102).

Chapter 3: System configuration fundamentals

This chapter describes the system configuration fundamentals for the Avaya Ethernet Routing Switch 4500 Series.

Hardware features

This section provides information about the hardware features of the Avaya Ethernet Routing Switch 4500 Series switch platforms.

Table 2: Hardware description by model

Model	Key Features
4526FX	24 100BaseFX ports (MTRJ connector) plus 2 10/100/1000 SFP combo ports Redundant power slot for DC/DC converter installation.
4526T	24 10/100BaseTX RJ-45 ports plus 2 10/100/1000/SFP combo ports Redundant power slot for DC/DC converter installation.
4526T-PWR	24 10/100BaseTX RJ-45 ports with PoE plus 2 10/100/1000/SFP combo ports Integrated redundant power connector for RPS 15 cable connection.
4550T	48 10/100BaseTX RJ-45 ports plus 2 10/100/1000 SFP combo ports Redundant power slot for DC/DC converter installation.
4550T-PWR	48 10/100BaseTX RJ-45 ports with PoE plus 2 10/100/1000 SFP combo ports Integrated redundant power connector for RPS 15 cable connection.
4524GT	24 10/100/1000Base TX RJ-45 ports and 4 shared SFP ports Redundant power slot for DC/DC converter installation.
4524GT-PWR	24 10/100/1000BaseTX RJ-45 ports with PoE and 4 shared SFP ports Integrated redundant power connector for RPS 15 cable connection.

Model	Key Features
4526GTX	24 10/100/1000BaseTX RJ-45 ports and 4 shared SFP ports plus 2 10GE XFP slots Redundant power slot for DC/DC converter installation.
4526GTX-PWR	24 10/100/1000BaseTX RJ-45 ports with PoE and 4 shared SFP ports plus 2 10GE XFP slots Integrated redundant power connector for RPS 15 cable connection.
4548GT	48 10/100/1000BaseTX RJ-45 ports and 4 shared SFP ports Redundant power slot for DC/DC converter installation.
4548GT-PWR	48 10/100/1000BaseTX RJ-45 with PoE and 4 shared SFP ports Integrated redundant power connector for RPS 15 cable connection.

Cooling fans

When you install the switch, always allow enough space on both sides for adequate air flow.

For more information about installation, see *Avaya Ethernet Routing Switch 4500 Series Installation* (NN47205-300).

Redundant power supply

The Avaya Ethernet Routing Switch 4500 Series Power over Ethernet (PoE) switches, Avaya Ethernet Routing Switch 4548GT-PWR, and Avaya Ethernet Routing Switch 4550T-PWR, can use an optional 470-Watt (W) Avaya Ethernet Routing Switch RPS 15 redundant power supply. The RPS 15 power supply chassis is two units high and can accommodate up to three RPS modules, each supporting up to four devices, to provide redundant power and uninterrupted operation in power failure. One RPS module connected to a PoE switch can provide up to 15.4 W for each port on all 48 ports. The RPS modules fit into the rear of the RPS 15 chassis. The UPS and associated battery pack module fit into the front of the chassis.

The non-PoE switches, Avaya Ethernet Routing Switch 4548GT, 4550T, and 4526FX, can use an optional 150W Avaya Ethernet Switch Power Supply Unit 10 and require the DC-DC Converter Module. The Avaya Ethernet Switch Power Supply Unit 10 provides scalable power redundancy and protection to low-wattage networking equipment. The PSU modules slide into the front of the Avaya Ethernet Routing Switch RPS 15 chassis.

DC-DC Converter Module

The DC-DC Converter Module for the non-PoE switches operates with the optional Avaya Ethernet Switch Power Supply Unit 15. The PoE switches do not require a DC-DC Converter Module.

The 100 W DC-DC Converter Module provides a Plug and Play redundant power supply unit for the Ethernet Routing Switch Series 4500 non-PoE switches. Contact your Avaya sales representative to order the converter module.

For further information about the DC-DC converter module, see *DC-DC Converter Module for the BayStack 5000 Series Switch* (215081-A).

Stacking capabilities

You can use the Avaya Ethernet Routing Switch 4500 Series switches in either of the following configurations:

- stand-alone
- stack

The Avaya Ethernet Routing Switch 4500 Series switches have a built-in cascade port to stack up to eight units. The cascade port provides an 40-Gigabit (Gb) cascading mechanism for the stacks.

A stack can consist of any combination of Avaya Ethernet Routing Switch 4500 Series switches.

Important:
All units in the stack must use the same software and diagnostic version.

To set up a stack, perform the following procedure.

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.

   Important:
   In a mixed stack of Avaya Ethernet Routing Switch 4500 switches, any switch type can act as the base unit.

Auto Unit Replacement

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. Because retained CFG images are kept in the DRAM of the stack, the stack power must be on during the procedure.

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 high 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 using ACLI. 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.

The ACLI command `show stack auto-unit-replacement` provides the following information:

```
Auto Unit Replacement  Auto-Restore:  Enabled Auto Unit Replacement Auto-Save:  Disabled

Unit #       Last Configuration-Save Time-Stamp    Ready For Replacement
1                    3 days 10:23:02                            Yes
2                    0 days 00:01:40                            No
3                    3 days 10:12:33                            Yes
6                    3 days 10:12:34                            No
8                    3 days 10:12:35                            Yes
```

Table 3: show stack auto-unit-replacement fields

Field	Definition
Auto Unit Replacement Auto-Restore	**Enable:** During a unit replacement, the configuration will be automatically restored to the new unit.
	Disable: During a unit replacement, the configuration will not be restored automatically.
Auto Unit Replacement Auto-Save	**Enable:** The current configuration of a unit in stack including base unit (if the stack is of 3 units or bigger) will be automatically saved to the base unit.
	Disable: The current configuration of a unit in stack including base unit (if the stack is of 3 units or bigger) will not be automatically saved to the base unit.
Last Configuration-Save Time-Stamp	The system-up time of the non base unit recorded when the non base unit sends configuration to the base unit.
Ready for Replacement	**Yes:** The current configuration of the non base unit is saved to the base unit. This unit is currently ready for replacement.
	No: The current configuration of the non base unit is not saved to the base unit. The latest changes of the configuration of the non base unit will be lost if the unit is replaced with a new unit.

For information about configuring AUR with ACLI, see Configuring AUR on page 105. For information about configuring AUR with Enterprise Device Manager (EDM), see Configuring AUR using EDM on page 226.

AUR function

The CFG mirror image is a duplicate CFG image (stored in the flash drive) 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.

CFG mirror image process

The CFG mirror image process is triggered by specific events.

Power Cycle

After a power cycle, all the CFG images in a stack are mirrored. Figure 1: CFG mirror process in stack on page 21 illustrates the CFG mirror images in a three-unit stack after the stack is powered on. Unit 1 is the Base Unit (BU) and all other units are Non-Based Units (NBU).

- Unit 1 (BU) contains mirror images for unit 2 (CFG 2) and unit 3 (CFG3).
- Unit 2 (NBU), is the TEMP-BU. It contains a mirror image of unit 1 (CFG1), in case the BU (unit 1) is removed from the stack.
- All three mirror images (CFG 1, CFG 2, and CFG 3) are active.
- Unit 2 is the AU of the CFG 2 mirror image.
- The Mac Address 2 is the AMA of the CFG2 mirror image.

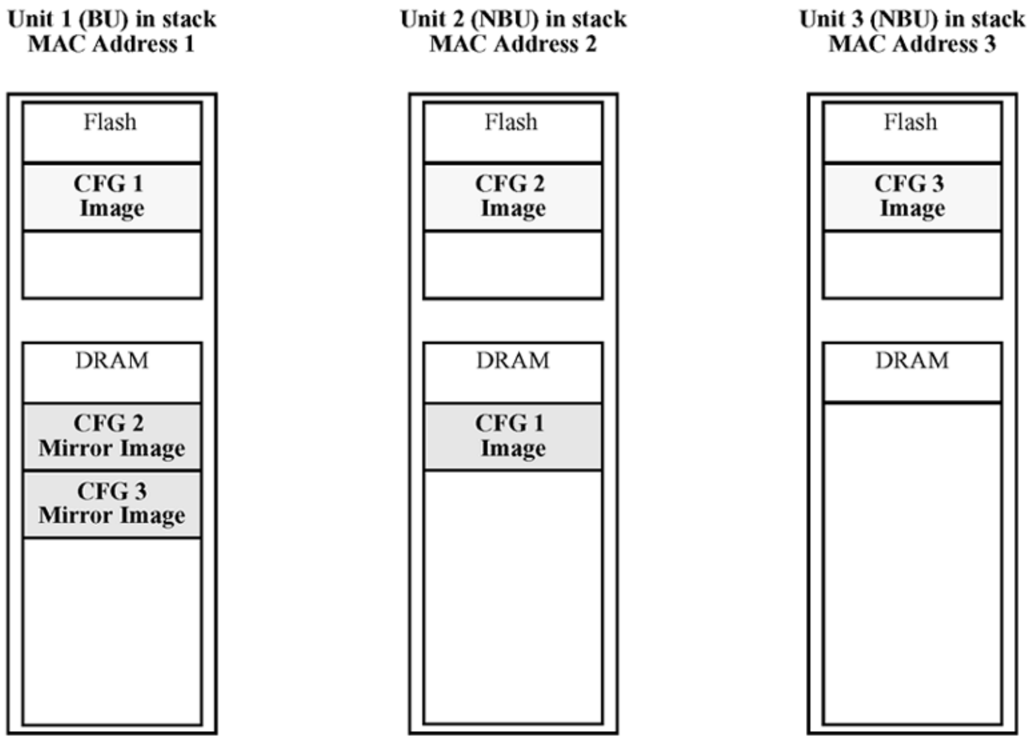


Figure 1: CFG mirror process in stack

Adding a unit

In a stack that has no any INACTIVE CFG mirror images, a new unit causes the CFG image of the new unit to be mirrored in the stack. For example, in Figure 2: CFG mirror images in the stack after adding unit 4 on page 22, after you add unit 4 to the stack, the CFG 4 mirror image is created in the BU (unit 1).

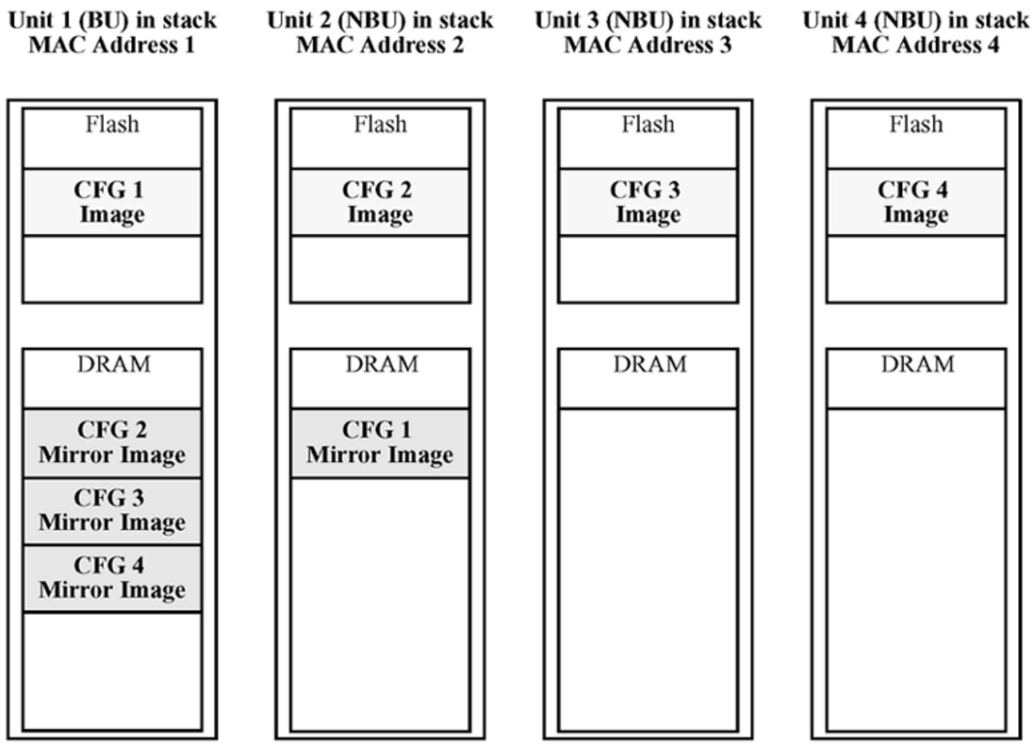


Figure 2: CFG mirror images in the stack after adding unit 4

Removing an NBU

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

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

For example, after you remove unit 4 from the stack shown in Figure 2: CFG mirror images in the stack after adding unit 4 on page 22, the CFG 4 mirror image becomes INACTIVE (see Figure 3: CFG mirror images after removing unit 4 on page 23). Another copy of the INACTIVE CFG 4 mirror image is also created in unit 2.

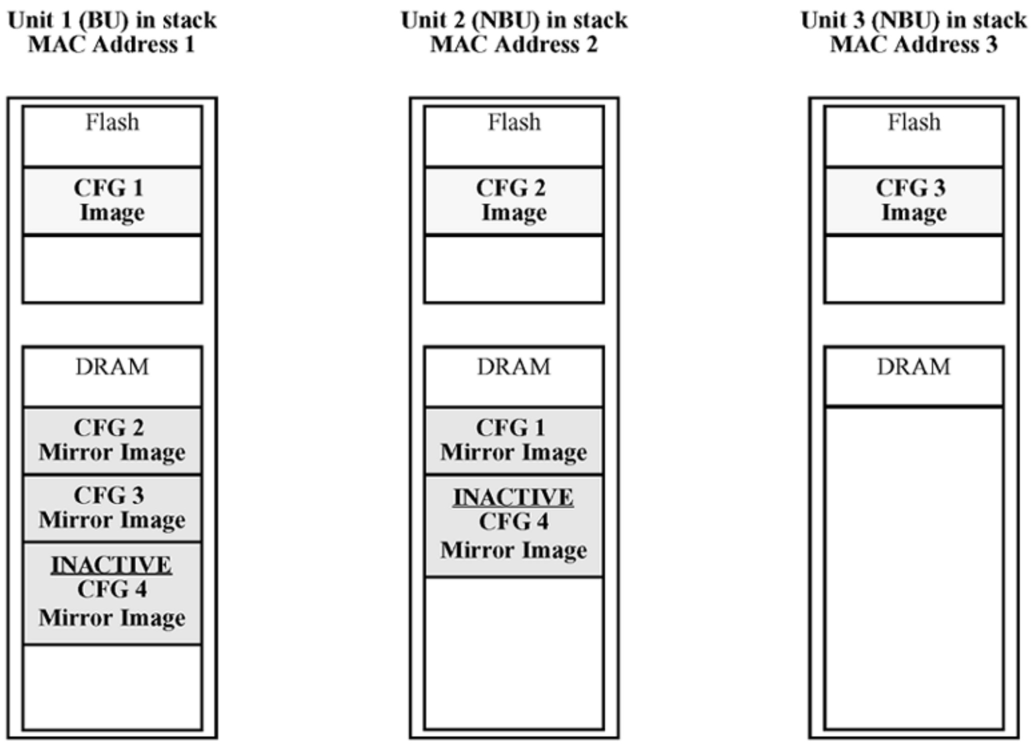


Figure 3: CFG mirror images after removing unit 4

Removing a BU

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

After you remove the BU from the stack shown in Figure 2: CFG mirror images in the stack after adding unit 4 on page 22, the TEMP-BU (unit 2) must mirror all the CFG images in the stack (see Figure 4: CFG mirror images in the stack after removing the BU (unit 1) on page 24). The feature also ensures that the stack always has two copies of an INACTIVE CFG mirror image.

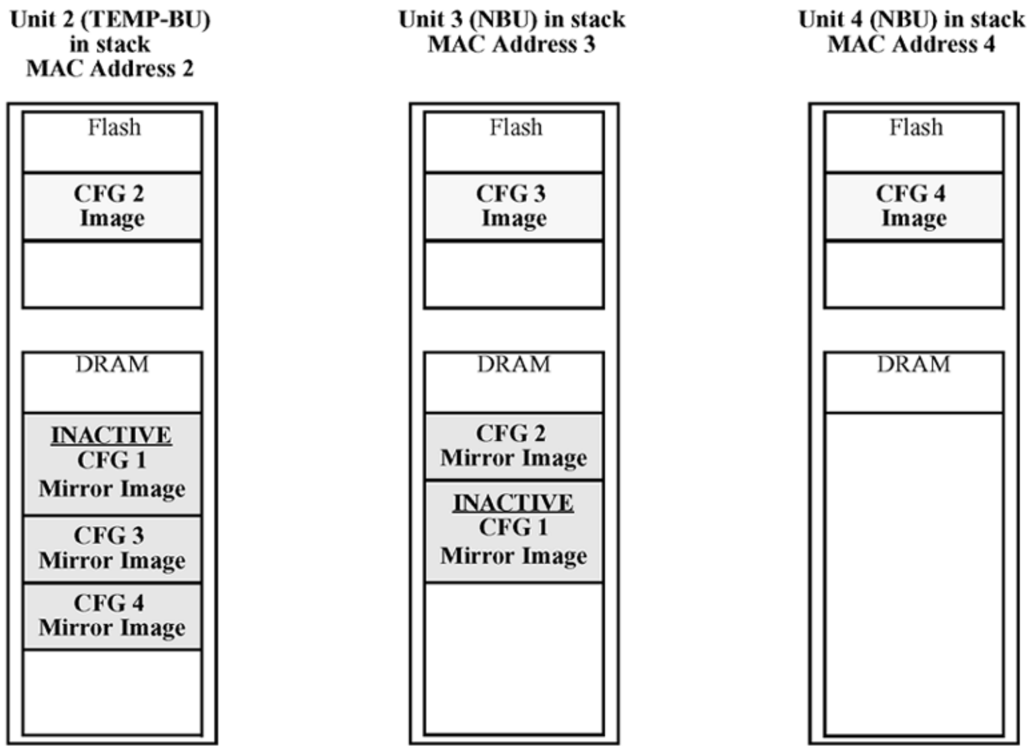


Figure 4: CFG mirror images in the stack after removing the BU (unit 1)

As shown in Figure 4: CFG mirror images in the stack after removing the BU (unit 1) on page 24

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

Restoring a CFG image

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

Important:

Restore a CFG image to a new unit happens only if you meet the following conditions.

- The AUR feature is enabled.
- At least one INACTIVE CFG mirror image exists in the stack.
- The MAC Address of the new unit is different from all the AMA of the INACTIVE CFG mirror images in the stack.

The image restore process consists of the following steps.

Add a new unit to a stack:

a. If more than one INACTIVE CFG mirror image is in the stack, select the one with the smallest unit ID for restoration.

b. Send the INACTIVE CFG mirror image in the stack to the new unit. The INACTIVE CFG mirror image becomes ACTIVE.

c. The new unit saves the received CFG image to the flash drive.

d. The new unit resets itself.

For example, if you add a unit 5 (MAC Address 5) to the stack shown in Figure 4: CFG mirror images in the stack after removing the BU (unit 1) on page 24, the following occurs (see Figure 5: CFG mirror images in the stack after adding unit 5 on page 26):

- The INACTIVE CFG 1 mirror image is copied to the CFG 5 image. Unit5 now has the configuration of unit 1, which is no longer in the stack.
- The INACTIVE CFG 1 mirror image in unit 2 becomes ACTIVE.
- The INACTIVE CFG 1 mirror image in unit 3 is removed.
- The MAC Address 5 of the unit 5 becomes the new AMA of the CFG1 mirror image.

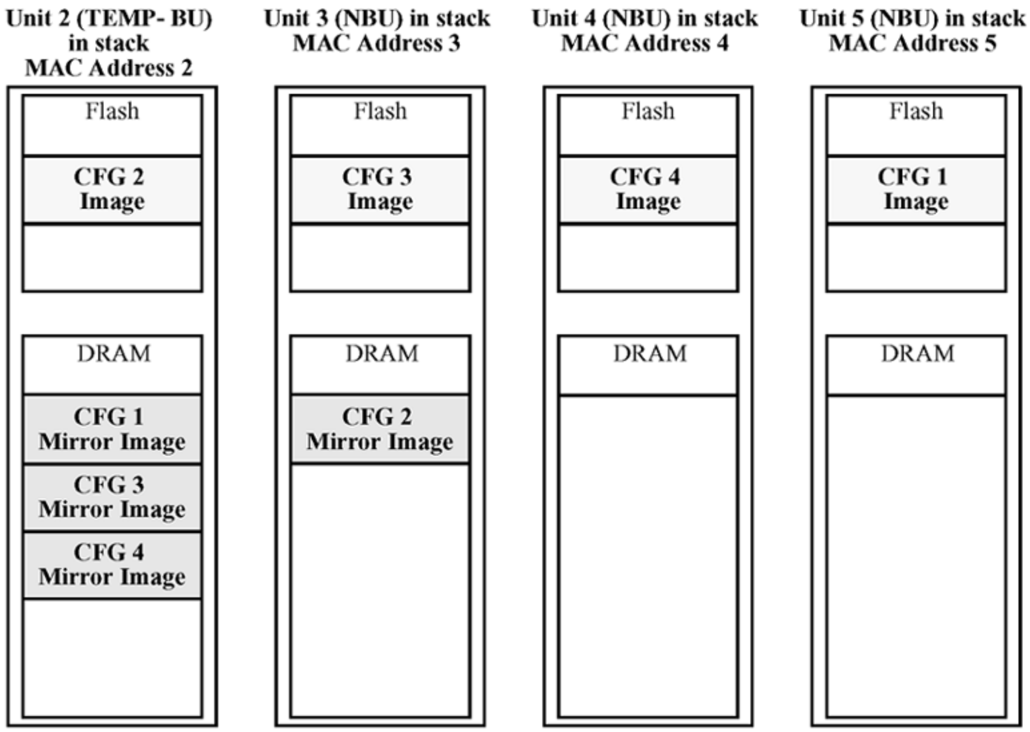


Figure 5: CFG mirror images in the stack after adding unit 5

Synchronizing the CFG mirror images with CFG images

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

Agent Auto Unit Replacement

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

Agent Auto Unit Replacement functions in the following manner:

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

Diagnostics AUR (DAUR)

Diagnostic Auto Unit Replacement (DAUR) enables the switch to update the diagnostic image of the non-base unit with the diagnostic image saved in the base unit of a stack. You must enable AAUR on the stack first.

Release 5.2 and up support DAUR. Previous software releases do not support DAUR.

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

The DAUR process starts when you enable AAUR if there is a stand-alone unit with a different diagnostic image connected to the stack. This process updates all the units in the stack.

When you enable or disable AAUR, you also enable or disable DAUR. The default for AAUR is enabled, so DAUR is also enabled by default.

There are no commands to separately enable or disable DAUR.

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

```
I 2 00:02:01:20 18 DAUR - Info: Receive request for diag image, start
transfer
```

```
I 2 00:02:01:22 19 DAUR - Info: Diag transfer finished
```

Add a unit to a stack

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

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

If you add a unit with the base unit select switch set to off to a unit with base unit select switch set, the non-base unit gets the diagnostic image from the base unit.

When the switch finishes the diagnostic image version update, the switch performs an AAUR check. If the new unit has the same agent image as the stack, the unit reboots. If the new unit has a different agent image, the switch performs an AAUR.

Note:

The new unit added on a stack must have an agent image with software release 5.1.0 or higher or AAUR and DAUR cannot upgrade the new unit.

The following table shows expected AAUR and DAUR behavior for different situations.

Table 4: Examples of AAUR and DAUR behavior in different situations

Stack master image and diagnostic version	Slave image diagnostic version	Expected behavior
Software 5.0/5.1 Diagnostic 5.0/5.1	Software 5.0/5.1 Diagnostic 5.0/5.1	Same image. Unit joins stack.
	Software 5.0/5.1 Diagnostic 5.2	Same image. Unit joins stack.
Software 5.0/5.1 Diagnostic 5.2	Software 5.2 Diagnostic 5.0/5.1	AAUR performed. AAUR downgrades the unit image and reboots the unit. The unit joins the stack after the reboot. No DAUR performed as DAUR is unavailable on 5.0/5.1
	Software 5.2 Diagnostic 5.2	
Software 5.2_SSH/non SSH Diagnostic 5.2	Software 5.0/5.1 Diagnostic 5.0/5.1	AAUR performed. AAUR upgrades the unit image then reboots the stack. DAUR upgrades the diagnostic image then reboots the unit. The unit joins the stack after the reboot.
	Software 5.0/5.1 Diagnostic 5.2	AAUR performed. AAUR upgrades the unit image then reboots the unit. Since the diagnostic images are the same, the unit joins the stack.
	Software 5.2_non SSH/SSH Diagnostic 5.1	Since the diagnostic and agent images are the different, DAUR upgrades the diagnostic image, and then AAUR transfers the agent. AAUR and DAUR reboot the unit. The unit joins the stack after the reboot.
	Software 5.2_non SSH/SSH Diagnostic 5.2	AAUR performs the agent image transfer and reboots the unit. The unit joins the stack after the reboot.

With version 5.2, when stack forced-mode is enabled and the base unit remains, Agent Auto Unit Replacement and Diagnostic Unit Replacement are working as explained on the preceding table.

Large image file

If the agent image size exceeds 6 Mb, the switch cannot perform the DAUR. The switch sends an error message to the base unit. You must perform a manual image upgrade or downgrade in this situation for both the diagnostic and agent images.

Stack Forced Mode

Stack Forced Mode allows one or both units to become stand-alone switches if a stack of two units breaks. The Stack Forced Mode allows you to manage one of the stand-alone devices from a broken stack of two with the previous stack IP address.

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 fails.

You can configure Stack Forced Mode through ACLI.

See Setting Stack Forced Mode on page 109 for procedures to set the Stack Forced Mode on a switch.

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). That allows an administrator to reach the device through an IP connection by telnet or EDM.

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

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

When a failure occurs in a stack of 2 units when forced stack mode is enabled, the previous non-base unit sends out a gratuitous ARP onto the management network. The purpose of sending out this gratuitous ARP is so that the non-base unit of a failed 2 unit stack can determine if the base unit is still operational and using the stack IP address. Such a failure situation in which both the base unit and non-base unit were operational, but not part of a stack could be possible if the 2 units in a stack were connected by a single stack cable and that stack cable were then 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 knows that the previous base unit is still operational and does not take over ownership of the stack IP address, but instead will use the local switch IP address if configured. If on the other hand the previous non-base unit does not receive a response from the previous base-unit; the previous non-base unit will now take over ownership of the stack IP address and issue a gratuitous ARP with it's own MAC address to ensure that all devices on the management VLAN have their ARP caches appropriately updated.

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

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

If the switch is in Stack Force mode and you want to set a switch 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, the switch will lose IPv6 connectivity to the switch. Avaya recommends that you change the settings with the Console Interface to switch or use an IPv4 address for management.

IPv6 management

This module provides information about the IPv6 management feature of the Avaya Ethernet Routing Switch 4500 Series switch platform.

IPv6 Management allows the user to configure an IPv6 address on the management VLAN. This enables IPv6 connectivity. The management VLAN can have both an IPv4 and an IPv6 address configured simultaneously (Avaya Ethernet Routing Switch 4500 functions as a dual stack network node).

There is no IPv6 routing support in the current phase and therefore only one IPv6 interface is associated to the management VLAN. You can only perform IPv6 interface configuration (enabling, assigning IPv6 address and prefix, changing other parameters, querying interface statistics) from ACLI or through SNMP (EDM).

IPv6 Management adds support for new standard MIBs (IP-MIB—RFC 4293, TCP-MIB—RFC 4022, UDP-MIB—RFC 4113) as well as the enterprise MIB rcIpv6.

If the switch is in Stack Force mode and you want to set a switch 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, the switch will lose IPv6 connectivity to the switch. Avaya recommends that you change the settings with the Console Interface to switch or use an IPv4 address for management.

The IPv6 header

The IPv6 header contains the following fields:

- a 4-bit Internet Protocol version number, with a value of 6
- an 8-bit traffic class field, similar to Type of Service in IPv4
- a 20-bit flow label that identifies traffic flow for additional Quality of Service (QoS)
- a 16-bit unsigned integer, the length of the IPv6 payload
- an 8-bit next header selector that identifies the next header
- an 8-bit hop limit unsigned integer that decrements by 1 each time a node forwards the packet (nodes discard packets with hop limit values of 0)
- a 128-bit source address
- a 128-bit destination address

IPv6 addresses

IPv6 addresses are 128 bits in length. The address identifies a single interface or multiple interfaces. IPv4 addresses, in comparison, are 32 bits in length. The increased number of possible addresses in IPv6 solves the inevitable IP address exhaustion inherent to IPv4.

The IPv6 address contains two parts: an address prefix and an IPv6 interface ID. The first 3 bits indicate the type of address that follows.

Figure 6: IPv6 address format on page 31 shows the IPv6 address format.

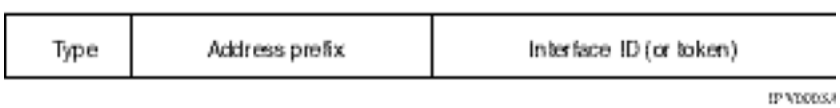


Figure 6: IPv6 address format

An example of a unicast IPv6 address is 1080:0:0:0:8:8000:200C:417A

Interface ID

The interface ID is a unique number that identifies an IPv6 node (a host or a router). For stateless autoconfiguration, the ID is 64 bits in length.

In IPv6 stateless autoconfiguration, the interface ID is derived by a formula that uses the link layer 48-bit MAC address. (In most cases, the interface ID is a 64-bit interface ID that contains the 48-bit MAC address.) The IPv6 interface ID is as unique as the MAC address.

If you manually configure interface IDs or MAC addresses (or both), no relationship between the MAC address and the interface ID is necessary. A manually configured interface ID can be longer or shorter than 64 bits.

Address formats

The format for representing an IPv6 address is n:n:n:n:n:n:n:n n is the hexadecimal representation of 16 bits in the address.

An example is as follows: FF01:0:0:0:0:0:0:43

Each nonzero field must contain at least one numeral. Within a hexadecimal field, however, leading zeros are not required.

Certain classes of IPv6 addresses commonly include multiple contiguous fields containing hexadecimal 0. The following sample address includes five contiguous fields containing zeroes with a double colon (::): FF01::43

You can use a double colon to compress the leading zero fields in a hexadecimal address. A double colon can appear once in an address.

An IPv4-compatible address combines hexadecimal and decimal values as follows: x:x:x:x:x:x:d.d.d.d x:x:x:x:x:x is a hexadecimal representation of the six high-order 16-bit pieces of the address, and d.d.d.d is a decimal representation of the four 8-bit pieces of the address.

For example: 0:0:0:0:0:0:13.1.68.3

or

::13.1.68.3

IPv6 extension headers

IPv6 extension headers describe processing options. Each extension header contains a separate category of options. A packet can include zero or more extension headers. For more information, see Figure 7: IPv6 header and extension headers on page 32.

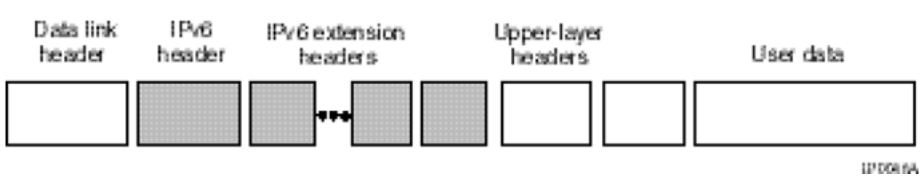


Figure 7: IPv6 header and extension headers

IPv6 examines the destination address in the main header of each packet it receives; this examination determines whether the router is the packet destination or an intermediate node in the packet data path. If the router is the destination of the packet, IPv6 examines the header extensions that contain options for destination processing. If the router is an intermediate node, IPv6 examines the header extensions that contain forwarding options.

By examining only the extension headers that apply to the operations it performs, IPv6 reduces the amount of time and processing resources required to process a packet.

IPv6 defines the following extension headers:

- The hop-by-hop extension header contains optional information that all intermediate IPv6 routers examine between the source and the destination.
- The end-to-end extension header contains optional information for the destination node.
- The source routing extension header contains a list of one or more intermediate nodes that define a path for the packet to follow through the network, to its destination. The packet source creates this list. This function is similar to the IPv4 source routing options.
- An IPv6 source uses the fragment header to send a packet larger than fits in the path maximum transmission unit (MTU) to a destination. In order to send a packet that is too large to fit in the MTU of the path to a destination, a source node can divide the packet into fragments and send each fragment as a separate packet, to be reassembled at the receiver.
- The authentication extension header and the security encapsulation extension header, used singly or jointly, provide security services for IPv6 datagrams.

Comparison of IPv4 and IPv6

The following table compares key differences between IPv4 and IPv6.

Table 5: IPv4 and IPv6 differences

Feature	IPv4	IPv6
Address length	32 bits	128 bits
IPsec support[1]	Optional	Required
QoS support	Limited	Improved
Fragmentation	Hosts and routers	Hosts only
Minimum MTU (packet size)	576 bytes	1280 bytes
Checksum in header	Yes	No
Options in header	Yes	No
Link-layer address resolution	ARP (broadcast)	Multicast Neighbor Discovery Messages

Feature	IPv4	IPv6
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router discovery[2]	Optional	Required
Uses broadcasts	Yes	No
Configuration[3]	Manual, DHCP	Manual

[1] Ethernet Routing Switch 4500 Series does not support IPsec.
[2] Ethernet Routing Switch 4500 Series does not perform Router discovery or advertise as a router.
[3] Ethernet Routing Switch 4500 Series does not implement any form of automatic configuration of IPv6 address in release 5.2.

ICMPv6

Internet Control Message Protocol (ICMP) version 6 maintains and improves upon features from ICMP for IPv4. ICMPv6 reports the delivery of forwarding errors, such as destination unreachable, packet too big, time exceeded, and parameter problem. ICMPv6 also delivers information messages such as echo request and echo reply.

Important:

ICMPv6 plays an important role in IPv6 features such as neighbor discovery, Multicast Listener Discovery, and path MTU discovery.

Neighbor discovery

IPv6 nodes (routers and hosts) on the same link use neighbor discovery (ND) to discover link layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided for IPv4 with the Address Resolution Protocol (ARP) and router discovery. Neighbor discovery replaces ARP in IPv6.

Hosts use ND to discover the routers in the network that you can use as the default routers, and to determine the link layer address of their neighbors attached on their local links. Routers also use ND to discover their neighbors and their link layer information. Neighbor discovery also updates the neighbor database with valid entries, invalid entries, and entries migrated to different locations.

Neighbor discovery protocol provides you with the following:

- Address and prefix discovery: hosts determine the set of addresses that are on-link for the given link. Nodes determine which addresses or prefixes are locally reachable or remote with address and prefix discovery.
- Router discovery: hosts discover neighboring routers with router discovery. Hosts establish neighbors as default packet-forwarding routers.

- Parameter discovery: host and routers discover link parameters such as the link MTU or the hop limit value placed in outgoing packets.
- Address autoconfiguration: nodes configure an address for an interface with address autoconfiguration.
- Duplicate address detection: hosts and nodes determine if an address is assigned to another router or a host.
- Address resolution: hosts determine link layer addresses (MAC for Ethernet) of the local neighbors (attached on the local network), provided the IP address is known.
- Next-hop determination: hosts determine how to forward local or remote traffic with next-hop determination. The next hop can be a local or remote router.
- Neighbor unreachability detection: hosts determine if the neighbor is unreachable, and address resolution must be performed again to update the database. For neighbors you use as routers, hosts attempt to forward traffic through alternate default routers.
- Redirect: routers inform the host of more efficient routes with redirect messages.

Neighbor discovery uses three components:

- host-router discovery
- host-host communication component
- redirect

For more information, see Figure 8: Neighbor discovery components on page 35 for the ND components.

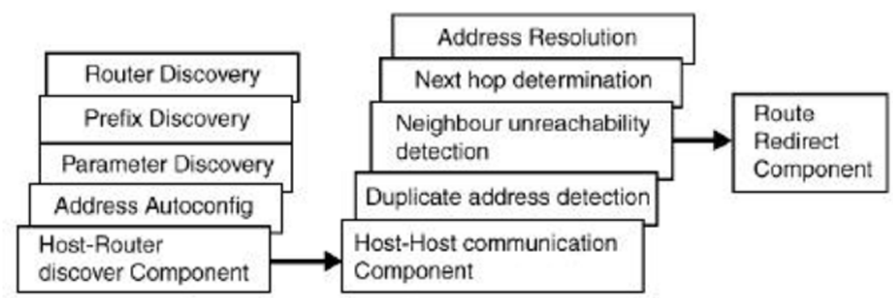


Figure 8: Neighbor discovery components

ND messages

The following table shows new ICMPv6 message types.

Table 6: IPv4 and IPv6 neighbor discovery comparison

IPv4 neighbor function	IPv6 neighbor function	Description
ARP Request message	Neighbor solicitation message	A node sends this message to determine the link-layer address of a neighbor or to

IPv4 neighbor function	IPv6 neighbor function	Description
		verify that a neighbor is still reachable through a cached link-layer address. You can also use neighbor solicitations for duplicate address detection.
ARP Reply message	Neighbor advertisement	A node sends this message either in response to a received neighbor solicitation message or to communicate a link layer address change.
ARP cache	Neighbor cache	The neighbor cache contains information about neighbor types on the network.
Gratuitous ARP	Duplicate address detection	A host or node sends a request with its own IP address to determine if another router or host uses the same address. The source receives a reply from the duplicate device. Both hosts and routers use this function.
Router solicitation message (optional)	Router solicitation (required)	The host sends this message upon detecting a change in a network interface operational state. The message requests that routers generate router advertisement immediately rather than at the scheduled time.
Router advertisement message (optional)	Router advertisement (required)	Routers send this message to advertise their presence together with various links and Internet parameters either periodically or in response to a router solicitation message. Router advertisements contain prefixes that you use for on-link determination or address configuration, and a suggested hop limit value.

IPv4 neighbor function	IPv6 neighbor function	Description
Redirect message	Redirect message	Routers send this message to inform hosts of a better first hop for a destination.

Neighbor discovery cache

The neighbor discovery cache lists information about neighbors in your network.

The neighbor discovery cache can contain the following types of neighbors:

- static: a configured neighbor
- local: a device on the local system
- dynamic: a discovered neighbor

The following table describes neighbor cache states.

Table 7: Neighbor cache states

State	Description
Incomplete	A node sends a neighbor solicitation message to a multicast device. The multicast device sends no neighbor advertisement message in response.
Reachable	You receive positive confirmation within the last reachable time period.
Stale	A node receives no positive confirmation from the neighbor in the last reachable time period.
Delay	A time period longer than the reachable time period passes since the node received the last positive confirmation, and a packet was sent within the last DELAY_FIRST_PROBE_TIME period. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME period of entering the DELAY state, neighbor solicitation is sent and the state is changed to PROBE.
Probe	Reachability confirmation is sought from the device every retransmit timer period.

The following events involve Layer 2 and Layer 3 interaction when processing and affect the neighbor cache:

- flushing the Virtual Local Area Network (VLAN) media access control (MAC)
- removing a VLAN
- performing an action on all VLANs
- removing a port from a VLAN
- removing a port from a spanning tree group (STG)
- removing a multi-link trunk group from a VLAN
- removing an Multi-Link Trunking port from a VLAN
- removing an Multi-Link Trunking port from an STG
- performing an action that disables a VLAN, such as removing all ports from a VLAN
- disabling a tagged port that is a member of multiple routable VLANs

Router discovery

IPv6 nodes discover routers on the local link with router discovery. The IPv6 router discovery process uses the following messages:

- Router advertisement
- Router solicitation

Router advertisement

Configured interfaces on an IPv6 router send out router-advertisement messages. Router-advertisements are also sent in response to router-solicitation messages from IPv6 nodes on the link.

Router solicitation

An IPv6 host without a configured unicast address sends router solicitation messages.

Path MTU discovery

IPv6 routers do not fragment packets. The source node sends a packet equal in size to the maximum transmission unit (MTU) of the link layer. The packet travels through the network to the source. If the packet encounters a link to a smaller MTU, the router sends the source node an ICMP error message containing the MTU size of the next link.

The source IPv6 node then resends a packet equal to the size of the MTU included in the ICMP message.

The default MTU value for a regular interface is 1500.

Flash memory storage

The sections in this module describe flash memory for software image upgrades.

Switch software image storage

The switch software image storage; uses flash memory to store the switch software image.

You can update the software image with a new version from flash memory.

You must have an in-band connection between the switch and the TFTP load host to the software image.

Important:
When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

Configuration parameter storage

All configuration parameters in the configuration parameter storage; are stored in flash memory.

These parameters are updated every 60 seconds if a change occurs, or upon execution of a reset command.

Important:
Do not power off the switch within 60 seconds of changing any configuration parameters.

If the switch is powered down within 60 seconds, any changes made to the configuration parameters can be lost.

Policy-enabled networking

With the policy-enabled networking, you can implement classes of services and assign priority levels to different types of traffic. You can also configure policies to monitor the characteristics of traffic.

For example, in policy-enabled networking, you can determine the sources, destinations, and protocols used by the traffic. You can also perform a controlling action on the traffic when certain user-defined characteristics match.

The policy-enabled networking; supports Differentiated Services (DiffServ). DiffServ is a network architecture through which service providers and enterprise network environments can offer various levels of services for different types of data traffic.

You can use DiffServ Quality of Service (QoS) to designate a specific level of performance on a packet-by-packet basis. If you have applications that require high performance and reliable service, such as voice and video over IP, you can use DiffServ to give preferential treatment to this data over other traffic.

Power over Ethernet

The Power over Ethernet; POE45GT; and the 4526GTX-PWR (PoE switches) provide IEEE 802.3af-compliant power or PoE on all 10/100/1000 RJ-45 ports.

The Power over Ethernet; 4526T-PWR and the 4550T-PWR (PoE switches) provide IEEE 802.3af-compliant power or PoE on all 10/100 RJ-45 ports.

PoE refers to the ability of the switch to power network devices over an Ethernet cable. Some of these devices include IP Phones, Wireless LAN Access Points, security cameras, and access control points.

The PoE switches automatically detect the network device requirements and dynamically supply the required DC voltage at a set current to each appliance.

To configure and manage the PoE features, you must use either ACLI or EDM.

Important:

You must use a four-pair Category 5 UTP cable for PoE. A standard two-pair UTP Cable does not support PoE.

Port mirroring

With port mirroring, also referred to as *conversation steering*, you can designate a single switch port as a traffic monitor for a specified port.

You can specify *port-based* mirroring for ingress and egress at a specific port, or address based mirroring, either source or destination. You also can attach a probe device, such as an Avaya StackProbe*, or equivalent, to the designated monitor port.

For more information about port mirroring, see *Avaya Ethernet Routing Switch 4500 Series Configuration — System Monitoring,* (NN47205-502).

Important:
Use ACLI to configure port mirroring.

Auto-MDI/X

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

When auto-MDI/X is active, any straight or crossover category 5 cable can provide connection to a port. If autonegotiation is disabled, auto-MDI/X is not active.

Auto-polarity

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

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 is reversed due to a wiring error. If autonegotiation is disabled, auto-polarity is not active.

Time Domain Reflectometer

The Time Domain Reflectometer (TDR), is used to test Ethernet cables connected to switch ports for defects (such as short pin and pin open), and display the results.

When you use the TDR to test a cable with a 10/100 MB/s link, the link is interrupted for the duration of the test and restored when the test is complete. Because ports that operate at slower speeds do not use all of the connected pins, test results for a port with a 10/100 MB/s link can be less detailed than test results for a port with a 1Gb/s link.

You can use the TDR to test cables from 5 to 120 meters in length with a margin of accuracy between 3 and 5 meters.

The TDR cannot test fibre optic cables.

Autosensing and autonegotiation

The Avaya Ethernet Routing Switch 4500 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 standard 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 occurs when the attached device cannot autonegotiate or uses 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 4500 Series reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the Avaya Ethernet Routing Switch 4500 Series, the ports negotiate down from 1000 Mb/s and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

Custom Autonegotiation Advertisements

In the Avaya Ethernet Routing Switch 4500 Series, you can use the Custom Autonegotiation Advertisements (CANA) feature to control the speed and duplex settings that each Ethernet port of the device advertises as part of the autonegotiation process.

Without CANA, a port with autonegotiation enabled advertises all speed and duplex modes supported by the switch and attempts to establish a link at the highest common speed and duplex setting. By using CANA, you can configure the port to advertise only certain speed and duplex settings, thereby establishing links only at these settings, regardless of the highest commonly supported operating mode.

CANA provides control over the IEEE802.3x flow control settings advertised by the port, as part of the autonegotiation process. You can set flow control advertisements to Symmetric, Asymmetric, or Disabled.

You may not want a port to advertise all supported speed and duplex modes in the following situations:

- If a network can support only a 10 Mb/s connection, you can configure a port to advertise only 10 Mb/s capabilities. Devices that uses autonegotiation to connect to this port connect at 10 Mb/s, even if both devices are capable of higher speeds.
- If you configure a port to advertise only 100 Mb/s full-duplex capability, the link becomes active only if the link partner can autonegotiate a 100 Mb/s full-duplex connection. This prevents mismatched speed or duplex settings if autonegotiation is disabled on the link partner.
- For testing or network troubleshooting, you can configure a link to autonegotiate at a particular speed or duplex mode.

Configuring CANA using ACLI

Use the **`auto-negotiation-advertisements`** command to configure CANA.

To configure port 5 to advertise the operational mode of 10 Mb/s and full duplex, enter the following command:

`auto-negotiation-advertisements port 5 10-full`

The following example displays sample output for the auto-negotiation-advertisements command to set port 5 to 10 Mb/s and full duplex.

auto-negotiation-advertisements command sample output

```
4548GT-PWR<config>#interface fastethernet 5
4548GT-PWR<config-if>#auto-negotiation-advertisements port 5 10-full
4548GT-PWR<config-if>#
```

Viewing current autonegotiation advertisements

To view the autonegotiation advertisements for the device, enter the following command:

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

The following example displays sample output for the show auto-negotiation-advertisements command after port 5 is set to 10 Mb/s and full duplex.

show auto-negotiation-advertisements command sample output

```
4548GT-PWR#show auto-negotiation-advertisements port 5
Unit/Port Autonegotiation Advertised Capabilities
--------- ----------------------------------------------------------------
1/5       10Full
```

Viewing hardware capabilities

To view the operational capabilities of the device, enter the following command:

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

The following example displays sample output for the show auto-negotiation-capabilities command for port 5.

show auto-negotiation-capabilities command sample output

```
4548GT-PWR#show auto-negotiation-capabilities port 1/5
Unit/Port Autonegotiation Capabilities
--------- ---------------------------------------------
1/5       10Full 10Half 100Full 100Half 1000Full
4548GT-PWR#
```

Setting default advertisements

To set default autonegotiation advertisements for the device, enter the following command in the Interface Configuration command mode:

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

To set default advertisements for port 5 of the device, enter the following command:

```
default auto-negotiation-advertisements port 5
```

The following example displays sample output for the default auto-negotiation-advertisements command to return port 5 to default auto-negotiation-advertisements status.

default auto-negotiation-advertisements command sample output

```
4548GT-PWR<config>interface fastethernet all
4548GT-PWR<config-if>#default-auto-negotiation-advertisements port 1/5
4548GT-PWR(config-if>#
```

Silencing advertisements

To set a port transmit no autonegotiation advertisements, enter the following command in the Interface Configuration command mode:

```
no auto-negotiation-advertisements [port <portlist>]
```

To silence the autonegotiation advertisements for port 5 of the device, enter the following command:

```
no auto-negotiation-advertisements port 5
```

The following example displays sample output for the no auto-negotiation-advertisements command to silence the auto-negotiation-advertisements for port 5.

no auto-negotiation-advertisements command sample output

```
4548GT-PWR<config-if>#no auto-negotiation-advertisements port 1/5
4548GT-PWR<config-if>#
```

ASCII configuration file

With the ASCII configuration file; you can download a user-editable ASCII configuration file from a TFTP server.

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

Load the ASCII configuration file automatically at boot time or on demand by using ACLI.

ACLI Command syntax :

```
4526GTX#script ?
```

```
run Run an ASCII configuration script
```

```
upload Upload the current ASCII configuration using an entry in the
ASCII configuration script table.
```

After you download the file, the configuration file automatically configures the switch or stack according to ACLI commands in the file.

With this feature, you can generate command configuration files that can be used by several switches or stacks with minor modifications.

The maximum size for an ASCII configuration file is 500 KB; split large configuration files into multiple files.

Use a text editor to edit the ASCII configuration. The command format is the same as that of ACLI.

Download the ASCII configuration file to the base unit by using ACLI commands. The ASCII configuration script completes the process.

Sample ASCII configuration file

This section shows a sample ASCII configuration file. This file is an example only and shows a basic configuration for a stand-alone switch that includes Multi-Link Trunking, VLANs, port speed and duplex, and SNMP configurations.

The following text represents a sample ASCII configuration file:

```
! --------------------------------------------------------
! example script to configure different features from ACLI
! --------------------------------------------------------
!
enable
configure terminal
!
!
! --------------------------------------------------------
! add several MLTs and enable
! --------------------------------------------------------
mlt 3 name seg3 enable member 13-14
mlt 4 name seg4 enable member 15-16
mlt 5 name seg5 enable member 17-18
!
!
! --------------------------------------------------------
! add vlans and ports
! --------------------------------------------------------
!
! create vlan portbased
vlan create 100 name vlan100 type port
!
! add Mlts created above to this VLAN
vlan members add 100 17
!
! create vlan ip protocol based
vlan create 150 name vlan150 type protocol-ipEther2
!
! add ports to this VLAN
! in this case all ports
vlan members add 150 ALL
vlan ports ALL priority 3
!
! igmp
! you could disable proxy on vlan 100
vlan igmp 100 proxy disable
!
! --------------------------------------------------------
! Examples of changing interface parameters
! --------------------------------------------------------
! change speed of port 3
interface Fastethernet 3
speed 10
duplex half
exit
!
! change speed of port 4
interface Fastethernet 4
speed auto
duplex auto
exit
!
!
! --------------------------------------------------------
! SNMP configuration
! --------------------------------------------------------
snmp-server host 192.168.100.125 private
snmp-server community private
!
!
exit
```

```
end
! ------------------------------------------------------
! Finished
! ------------------------------------------------------
```

Important:

To add comments to the ASCII configuration file, add an exclamation point (!) to the beginning of the line.

ASCII Download Enhancements

The purpose of the ASCII Download Log feature is to log all the failed commands from the ASCII configuration file as informational customer messages.

1. `Connection error` (ACG_DOWNLOAD_ERROR)

   The message describes the situation in which the connection failed, therefore the ASCII Configuration File could not be accessed or used. The IP and the filename will be in the message in case of a TFTP server usage, or the filename in case of a USB usage. The message also contains the cause of the error the same as the one displayed to the CLI. An ACG_DOWNLOAD_ERROR error message is logged only in the following situations:

   - Transfer Timed Out
   - Invalid TFTP Server address
   - File not found
   - Configuration failed
   - Switch IP not set
   - Stack IP not set
   - TFTP Server address not set
   - Mask not set
   - File too large
   - Invalid Configuration File
   - Invalid Configuration File or File not found
   - Error accessing USB/ASCII file

   Note:

   It doesn't matter from which interface we start the ASCII file download, the logged message will be the ones from the CLI.

   Example message for TFTP server usage:

Type	Unit	Time	Idx Src	Message
----	----	------------	------	---------------
I	1	00:00:00:30	5	ASCII transfer failed, Addr: 10.3.2.137, File: config.txt. File not found.

Example message for USB usage:

Type	Unit	Time	Idx Src	Message
----	----	------------	------	---------------
I	1	00:00:00:30	6	ASCII transfer failed, from USB, File: config.txt. Error accessing USB/ASCII file.

2. `Connection error on load on boot` (ACG_DOWNLOAD_ERROR_ON_BOOT)

   The message describes the situation in which the connection failed at load on boot, therefore the ASCII Configuration File could not be accessed or used. The IP and the filename will be in the message in case of a TFTP server usage, or the filename in case of a USB usage. The message also contains the cause of the error the same as the one displayed to the CLI. There are some cases in which the IP number is unknown, therefore the “?” sign will be used.

   Example message for TFTP server usage:

Type	Unit	Time	Idx Src	Message
----	----	------------	------	---------------
I	1	00:00:00:30	5	ASCII transfer failed at load on boot, Addr: 10.3.2.137, File: config.txt. File not found.

   Example message for USB usage:

Type	Unit	Time	Idx Src	Message
----	----	------------	------	---------------
I	1	00:00:00:30	6	ASCII transfer failed at load on boot, from USB, File: config.txt. Error accessing USB/ASCII file.

3. `Connection OK` (ACG_DOWNLOAD_OK)

   The message describes the situation in which the connection was successful, the ASCII Configuration File could be accessed and it can be used. The IP and the filename will be in the message in case of a TFTP server usage, or the filename in case of a USB usage.

   Example message for TFTP server usage:

Type	Unit	Time	Idx Src	Message
----	----	------------	------	---------------
I	1	00:00:00:45	10	ASCII transfer OK, Addr: 10.3.2.137, Filename: config.txt

   Example message for USB usage:

Type	Unit	Time	Idx Src	Message
----	----	------------	------	---------------
I	1	00:00:00:45	10	ASCII transfer OK, from USB, Filename: config.txt

4. `Connection OK on load on boot` (ACG_DOWNLOAD_OK_ON_ BOOT)

   The message describes the situation in which the connection was successful at load on boot, the ASCII Configuration File could be accessed and it can be used. The IP and the filename will be in the message in case of a TFTP server usage, or the filename in case of a USB usage.

   Example message for TFTP server usage:

```
                              Idx
Type   Unit   Time            Src     Message

----   ----   ------------    ------  ---------------
I      1      00:00:00:45     10      ASCII transfer OK
                                      at load on boot,
                                      Addr: 10.3.2.137,
                                      Filename:
                                      config.txt
```

Example message for USB usage:

```
                              Idx
Type   Unit   Time            Src     Message

----   ----   ------------    ------  ---------------
I      1      00:00:00:45     10      ASCII transfer OK
                                      at load on boot,
                                      from USB,
                                      Filename:
                                      config.txt
```

5. `Execution OK` (ACG_EXECUTION_OK)

   The message describes the situation in which the execution of the ASCII Configuration File was successful, no error occurred at any line.

   Example message for both TFTP server usage and USB usage:

```
                              Idx
Type   Unit   Time            Src     Message

----   ----   ------------    ------  ---------------
I      1      00:00:00:45     10      ASCII finished
                                      successfully.
```

6. `Execution OK on load on boot` (ACG_EXECUTION_OK_ON_ BOOT)

   The message describes the situation in which the execution of the ASCII Configuration File was successful at load at boot, no error occurred at any line.

   Example message for both TFTP server usage and USB usage:

```
                              Idx
Type   Unit   Time            Src     Message

----   ----   ------------    ------  ---------------
I      1      00:00:00:45     10      ASCII finished
```

```
successfully at
load on boot.
```

7. `Failed command` (ACG_CMD_ERR)

    The message describes the situation in which a command from the ASCII Configuration File failed. The failed command text line number will be in the message. In the case that the cause of the error is one of the following, the cause will also be in the message: “Invalid input detected”, “Ambiguous command”, “Incomplete command”, “Permission denied”, “Not allowed on slave”. In other words, if one of these messages is displayed in the CLI, it will be in the ASCII_CMD_ERR message.

    Note:
    In some cases, the ASCII file download is programmed to stop when the first error is found. Therefore, only this error will be logged.

    Example error message:

```
                                    Idx
Type    Unit    Time                Src     Message
----    ----    ------------        ------  ---------------
I       1       00:00:09:33         21      ASCII failed at
                                            line 4. Invalid
                                            input detected.
```

Backup configuration file

When the switch writes a configuration file to FLASH, the switch writes to the primary configuration block, updates the CRC16 checksum in the multi configuration area, and then saves the information to the auxiliary configuration block. This prevents the corruption of the configuration file if power failure occurs during the write process.

When you boot the switch, if the switch detects corruption in the primary configuration file (checksum mismatch), the switch sends a message to the system log. The switch then attempts to load the secondary configuration file from the auxiliary configuration block if the checksum is correct, and then sends a message to the system log. If both primary and auxiliary configurations blocks are corrupted, the switch resets the settings to default and sends a message to the system log.

The auxiliary configuration block is a mirror of the active configuration block. The backup configuration feature is transparent to the user.

You can check the system log for messages if you suspect corruption in a configuration file.

This feature is enabled by default. There are no configuration commands for this feature.

Displaying unit uptime

You can display the uptime for each unit in a stack. Unit stack uptime collects the stack uptime for each unit in a stack and reports this information when requested. You can determine how long each unit is connected to the stack. You can use ACLI commands to display the unit uptimes.

Port naming

You can name or specify a text string for each port. This feature provides easy identification of the connected users.

Use ACLI or EDM to name ports.

Port error summary

You can view all ports that have errors in an entire stack.

If a particular port has no errors, it is not displayed in the port error summary.

IP address for each unit in a stack

You can assign an IP address to each unit in a stack. Use ACLI to configure the IP addresses for each unit within a stack.

BootP mode

The Avaya Ethernet Routing Switch 4500 Series supports the Bootstrap protocol (BootP).

You can use BootP to retrieve an ASCII configuration file name and configuration server address.

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

The Avaya Ethernet Routing Switch 4500 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 4500 Series BootP requests.

The BootP modes supported by the Avaya Ethernet Routing Switch 4500 Series are

- BootP or Last Address mode
- BootP-When-Needed
- BootP Always
- BootP Disabled

Important:
The default BootP mode is BootP-When-Needed.

DHCP client

The Dynamic Host Configuration Protocol (DHCP) client, uses either DHCP or BootP to assign an IPv4 address to the management VLAN. Using the DHCP client, the switch can retrieve IP address, netmask, default gateway, and Domain Name Server (DNS) information for a maximum of three DNS servers.

Web Quick Start

You can use the Web Quick Start feature to enter the setup mode through a single screen.

This feature is supported only by the Web interface.

During the initial setup mode, all ports in the switch or stack are assigned to the default VLAN.

You can use the Web Quick Start screen to configure the following information:

- stack IP address
- subnet mask
- default gateway
- SNMP Read community

- SNMP Write community
- Quick Start VLAN

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.

Clocks use NTP to synchronize to a few milliseconds, depending on the clock source and local clock hardware.

SNTP synchronizes the Universal Coordinated Time (UTC) to accuracy within 1 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.

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 can use the broadcast and multicast modes.

SNTP accuracy is typically in the order of significant fractions of a second. This accuracy correlates to the latencies between the SNTP client device and the NTP server. In a low-latency network, the SNTP accuracy can be reduced to less than a 100 millisecond range and, to further increase the accuracy, you can use a simple latency measurement algorithm.

The intended accuracy for this implementation is 1 second, which is sufficient for logs and time displays on UIs.

When SNTP is enabled (the default value is Disabled), the system synchronizes with the configured NTP server at boot-up (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. It 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 5 minutes between each retry.

Ping enhancement

Using ACLI you can specify additional ping parameters, including the number of ICMP packets to be sent, the packet size, the interval between packets, and the timeout. You can also set ping to continuous, or you can set a debug flag to obtain extra debug information.

For more information about ping command, see ping command on page 159.

New unit Quick configuration

In Software Release 5.2, the New Unit Quick Configuration feature, you can create a default configuration to apply to any new unit entering a stack configuration. You can add new units to the stack without resetting the stack.

For more information about New Unit Quick Configuration, see *Avaya Ethernet Routing Switch 4500 Series Installation Guide* (NN47205-300).

Updating switch software

Updating switch software is a necessary part of switch configuration and maintenance. You can update the version of software running on the switch through either EDM or ACLI.

Before you attempt to change the switch software, ensure that the following prerequisites are in place:

- The switch has a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is on the network that is accessible by the switch and that has the desired software version loaded.
- If you change the switch software on a an Avaya Ethernet Routing Switch 4524GT-PWR or Avaya Ethernet Routing Switch 4548GT-PWR using a USB Mass Storage Device, ensure that the Mass Storage Device has the desired software version and is inserted into the front panel USB port.
- If you use ACLI, ensure that ACLI is in Privileged EXEC mode.
- If you use EDM, ensure that SNMP is enabled.

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

See the following sections for details about updating switch software:

• Managing switch software using EDM on page 240
• LED activity during software download on page 56

LED activity during software download

During the software download, the port LEDs light one after another in a chasing pattern, except for ports 35, 36, 47, and 48 on an Avaya Ethernet Routing Switch 4548GT.

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.

Asset ID string configuration

You can define an Asset ID, which provides inventory information for the switch, stack or each unit within a stack. An asset ID consists of an alphanumeric string up to 32 characters in length for the switch or stack. An Asset ID is useful for recording your company specific asset tracking information, such as an asset tag affixed to the switch. The Avaya Ethernet Routing Switch 4500 allows you to configure the asset-ID by ACLI commands and EDM.

Agent and diagnostic software status display

You can display the currently loaded and operational switch or stack software status for both agent and diagnostic loads. With the `show boot` ACLI command and variables, you can view the agent or diagnostic load status individually, or together. The Boot Image, EDM tab displays agent and diagnostic load status information together.

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 multiple specific time periods. These time periods (a maximum of 42) can be a as short as one minute, or last a complete week, complete weekend, or individual days.

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.

Table 8: Energy savings

Switch model	Typical power consumption in Normal Mode (in watts)	Typical power consumption in Energy Saver (in watts)	Savings per switch (in Watts)	Savings per port (in Watts)
4548GT	103	63	40	0.83
4548GT-PWR [1]	98	58	40	0.83
4524GT	68	45	23	0.96
4524GT-PWR [1]	62	41	21	0.87
4526GTX	76	53	23	0.96
4526GTX-PWR[1]	71	49	22	0.91
4526T	43	37	6	0.25
4526T-PWR[1]	40	35	5	0.2
4550T	50	40	10	0.21
4550T-PWR[1]	55	45	10	0.21
4526FX[1]	63	61	2	1
[1]The power consumption values in this table can vary by up to 10%. Power consumption values can differ if a switch operates at different voltages. Power supplies operating at higher voltages are generally more efficient.				

Chapter 4: Power over Ethernet

The Avaya Ethernet Routing Switch 4500 Series 4548GT-PWR and the 4526GTX-PWR (PoE switches) provide IEEE 802.3af-compliant power or PoE on all 10/100/1000 RJ-45 ports.

The Avaya Ethernet Routing Switch 4500 Series 4526T-PWR and the 4550T-PWR (PoE switches) provide IEEE 802.3af-compliant power or PoE on all 10/100 RJ-45 ports.

PoE is based on the IEEE 802.3af standard.

PoE is the ability of the 4550T-PWR,4548GT-PWR,4526T-PWR and 4526GTX-PWR to power network devices over the Ethernet cable. These devices include IP Phones, wireless LAN access points, security cameras, and access control points.

For more information about power supplies, see *Avaya Ethernet Routing Switch 4500 Series Installation* (NN47205-301).

You can configure PoE from ACLI, SNMP, Enterprise Device Manager (EDM). For details, see the following sections.

- PoE overview on page 59
- Port power priority on page 60

To configure PoE, see the following procedures:

- Configuring PoE using ACLI on page 125
- PoE configuration for switch ports using EDM on page 234
- Switch unit PoE management using EDM on page 215

PoE overview

The Avaya Ethernet Routing Switch 4500 Series 4550T-PWR, 4548GT-PWR,4526T-PWR and 4526GTX-PWR are ideal to use with Avaya Business Communication Manager system, IP phones, hubs, and wireless access points. You can use these switches with all network devices.

By using the Avaya Ethernet Routing Switch 4500 Series 4550T-PWR,4548GT-PWR, 4526T-PWR and 4526GTX-PWR you can plug any IEEE802.3af-compliant powered device into a front-panel port and receive power in that port. Data also can pass simultaneously on that port. This capability is called PoE.

For more information about PoE and power supplies, see *Avaya Ethernet Routing Switch 4500 Series Installation* (NN47205-301).

The IEEE 802.3af draft standard regulates a maximum of 15.4 W of power for each port; that is, a power device cannot request more than 15.4 W of power. As different network devices require different levels of power, the overall available power budget of the switch; depends on your power configuration and the particular connected network devices. If you connect an IP device that requires more than 16 W of power, you see an error on that port notifying you of an overload.

The Avaya Ethernet Routing Switch 4500 Series 4550T-PWR,4548GT-PWR, 4526T-PWR and 4526GTX-PWR automatically detect each IEEE 802.3af-draft-compliant powered device attached to each front-panel port and immediately sends power to that appliance. The switches also automatically detect how much power each device requires and supply the required DC voltage at a set current based on the load conditions and current availability. The switches support both PoE and standard LAN devices.

The power detection function of the Avaya Ethernet Routing Switch 4500 Series 4550T-PWR,4548GT-PWR, 4526T-PWR and 4526GTX-PWR operate independently of the data link status. A device that is already operating the link for data or a device that is not yet operational can request power. That is, the switches provide power to a requesting device even if the data link for that port is disabled. The switches monitor the connection and automatically disconnect power from a port when you remove or change the device, as well as when a short occurs.

The switches automatically detect devices that require no power connections from them, such as laptop computers or other switching devices, and send no power to those devices. You control the supply of power to specific ports by setting the maximum allowed power to each port in 1 W increments, from 3 W to 16 W.

Important:

Allow 30 seconds between unplugging and replugging an IP device to the switch to enable the IP device to discharge. If you attempt to connect earlier, the switch may not detect the IP device.

The Avaya Ethernet Routing Switch 4500 provides the capability to set a PoE power threshold, which lets you set a percentage of the total PoE power usage at which the switch sends a warning trap message. If the PoE power usage exceeds the threshold and SNMP traps are appropriately configured, the switch sends the **pethMainPowerUsageOnNotification** trap. If the power consumption exceeds and then falls below the threshold, the switch sends the **pethMainPowerUsageOffNotification** trap.

Port power priority

You can configure the power priority of each port by choosing low, high, or critical power priority settings.

The switch automatically drops low-priority ports when the power requirements exceed the available power budget. When the power requirements becomes lower than the switch power budget, the power returns to the dropped port. When several ports have the same priority, one of them must be dropped. In this case, the port with the highest port number is dropped.

For example, assume the following scenario:

- Ports 1 to 40 are configured as low priority.
- Port 41 is configured as high priority.
- Ports 1 to 40 are connected to powered devices.

The devices connected to the ports consume the available Avaya Ethernet Routing Switch 4500 Series 4550T-PWR,4548GT-PWR, 4526T-PWR and 4526GTX-PWR switch power.

The device connected to port 41 requests power from the Avaya Ethernet Routing Switch 4550T–PWR or the Avaya Ethernet Routing Switch 4548GT–PWR. The switch provides the required power as port 41 is configured as high priority. However, to maintain the power budget, the switch drops one of the ports configured as low priority. In this case, the switch drops power to port 40 and provides power to port 41. If another port drops power, the system automatically reinstates power to port 40.

Viewing PoE ports using EDM

The front panel view of Enterprise Device Manager (EDM) provides additional information for PoE ports on the Avaya Ethernet Routing Switch 4548GT–PWR. This additional information is in the form of a colored P that appears inside the graphic representation of the port. This colored P represents the current power aspect of the PoE port.

Table 9: Power Aspect color codes on page 61 explains the different colors displayed by the power aspect.

Table 9: Power Aspect color codes

Color	Description
Green	The port is currently delivering power.
Red	The power and detection mechanism for the port is disabled.
Orange	The power and detection mechanism for the port is enabled. The port is not currently delivering power.
White/Gray	The power and detection mechanism for the port is unknown.

Important:

The data and power aspect coloring schemes are independent of each other. You can view the initial status for both data and power aspect for the port. To refresh the power status, right-click the unit, and select Refresh PoE Status from the shortcut menu.

Chapter 5: Link Layer Discovery Protocol (802.1ab)

This chapter describes the Link Layer Discovery Protocol (LLDP) (IEEE 802.1ab) and contains the following topics:

Link Layer Discovery Protocol (IEEE 802.1AB) Overview on page 63

See the following sections for the procedures to configure LLDP:

- Configuring LLDP using ACLI on page 164
- LLDP configuration using EDM on page 284

Link Layer Discovery Protocol (IEEE 802.1AB) Overview

From Release 5.1 and on, switch software supports the Link Layer Discovery Protocol (LLDP) (IEEE 802.1AB), which enables stations connected to a LAN to advertise their capabilities to each other, enabling the discovery of physical topology information for network management. LLDP-compatible stations can consist of any interconnection device including PCs, IP Phones, switches, and routers. Each LLDP station stores LLDP information in a standard Management Information Base (MIB), making it possible for a network management system (NMS) or application to access the information.

Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with 4500 Series).
- receives network management information from adjacent stations on the same LAN.

LLDP also makes it possible to discover certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers. For example, it can be used to discover duplex mismatches between an IP Phone and the connected switch.

LLDP is compatible with IETF PROTO MIB (IETF RFC 2922).

Figure 9: LLDP How it works on page 64 shows an example of how LLDP works in a network.

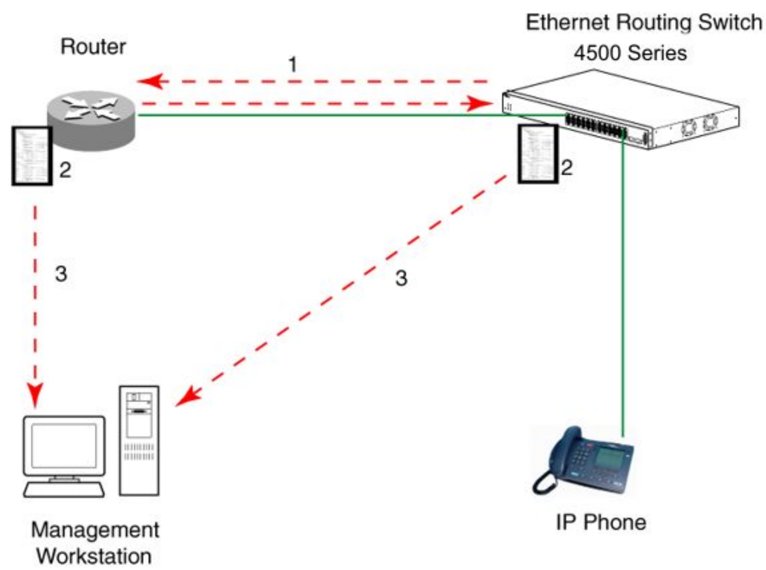


Figure 9: LLDP How it works

1. The Ethernet Routing Switch and LLDP-enabled router advertise chassis/port IDs and system descriptions to each other.
2. The devices store the information about each other in local MIB databases, accessible by using SNMP.
3. A network management system retrieves the data stored by each device and builds a network topology map.

LLDP operational modes

LLDP is a one-way protocol. An LLDP agent can transmit information about the capabilities and current status of the system associated with its MAC service access point (MSAP) identifier. The LLDP agent also can receive information about the capabilities and current status of the system associated with a remote MSAP identifier. However, LLDP agents cannot solicit information from each other.

You can set the local LLDP agent to transmit only, receive only, or to both transmit and receive LLDP information. You can configure the state for LLDP reception and transmission using SNMP or ACLI commands.

Connectivity and management information

The information fields in each LLDP frame are in a Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of short, variable length information elements known as TLVs (type, length, value).

Each LLDPDU includes the following four mandatory TLVs:

- **Chassis ID TLV**
- **Port ID TLV**
- **Time To Live TLV**
- **End Of LLDPDU TLV**

The chassis ID and the port ID values are concatenated to form a logical MSAP identifier that the recipient uses to identify the sending LLDP agent and port.

A non-zero value in the Time to Live (TTL) field of the TTL TLV indicates to the receiving LLDP agent how long the LLDPDU information from the MSAP identifier remains valid. The receiving LLDP agent automatically discards all LLDPDU information, if the sender fails to update it in a timely manner. A zero value in TTL field of Time To Live TLV tells the receiving LLDP agent to discard the information associated with the LLDPDU MSAP identifier.

From Release 5.1 and on, in addition to the four mandatory TLVs, switch software supports the TLV extension set consisting of Management TLVs and organizationally-specific TLVs. Organizationally-specific TLVs are defined by either the professional organizations or the individual vendors that are involved with the particular functionality being implemented. You can specify which of these optional TLVs to include in the transmitted LLDPDUs for each port.

For more information about the supported TLV extension set, see the following:

- Basic management TLV set on page 65
- IEEE 802.1 organizationally-specific TLVs on page 66
- IEEE 802.3 organizationally-specific TLVs on page 66

Basic management TLV set

The basic management TLV set contains the following TLVs:

- **Port Description TLV**
- **System Name TLV**
- **System Description TLV**
- **System Capabilities TLV** (indicates both the capabilities and current primary network function of the system, such as end station, bridge, or router)
- **Management Address TLV**

Beginning with Release 5.5 the switch supports IPv4 and IPv6 management addresses and the transmission of all TLVs from the basic management TLV set is enabled by default.

IEEE 802.1 organizationally-specific TLVs

The optional IEEE 802.1 organizationally-specifc TLVs are:

- **Port VLAN ID TLV** contains the local port PVID.
- **Port And Protocol VLAN ID TLV** contains the VLAN IDs of the port and protocol VLANs that contain the local port.
- **VLAN Name TLV** contains the VLAN names of the VLANs that contain the local port.
- **Protocol Identity TLV** advertises the protocol supported. The following values are used for supported protocols on the 4500 Series:
  - Stp protocol {0x00,0x26,0x42,0x42,0x03, 0x00, 0x00, 0x00}
  - Rstp protocol string {0x00,0x27,0x42,0x42,0x03, 0x00, 0x00, 0x02}
  - Mstp protocol string {0x00,0x69,0x42,0x42,0x03, 0x00, 0x00, 0x03}
  - Eap protocol string {0x88, 0x8E, 0x01}
  - Lldp protocol string {0x88, 0xCC}

IEEE 802.3 organizationally-specific TLVs

The optional IEEE 802.3 organizationally-specifc TLVs are:

- **MAC/PHY Configuration/Status TLV** indicates the autonegotiation capability and the speed and duplex status of IEEE 802.3 MAC/PHYs.
- **Power-Via-MDI TLV** indicates the capabilities and current status of IEEE 802.3 PMDs that either require or can provide power over twisted-pair copper links.
- **Link Aggregation TLV** indicates the current link aggregation status of IEEE 802.3 MACs.
- **Maximum Frame Size TLV** indicates the maximum supported 802.3 frame size.

Organizationally-specific TLVs for MED devices

The optional organizationally-specific TLVs for use by Media Endpoint Devices (MED) and MED network connectivity devices are:

- **Capabilities TLV** enables a network element to advertise the LLDP-MED TLVs it is capable of supporting.
- **Network Policy Discovery TLV** is a fixed length TLV that enables both network connectivity devices and endpoints to advertise VLAN type, VLAN identifier (VID), and Layer 2 and Layer 3 priorities associated with a specific set of applications on a port. In

addition, an LLDP-MED endpoint advertises this TLV for supported application types to enable the discovery of specific policy information and the diagnosis of network policy configuration mismatch issues.

- **Location Identification TLV** allows network connectivity devices to advertise the appropriate location identifier information for an endpoint to use in the context of location-based applications. The Location Identification Discovery extension enables the advertisement of location identifier information to Communication Endpoint Devices (Class III), based on the configuration of the Network Connectivity Device to which it is connected. This is expected to be related to wiremap or similar network topology data, such that the configuration of the Network Connectivity Device can uniquely identify the physical location of the connected MED Endpoint, and hence the correct location identifier information for it to use.
- **Extended Power-via-MDI TLV** enables advanced power management between an LLDP-MED endpoint and network connectivity devices. The Extended Power-via-MDI TLV enables the advertisement of fine grained power requirement details, endpoint power priority, and power status for both endpoint and network connectivity devices.
- **Inventory TLVs** are important in managed VoIP networks. Administrative tasks in these networks are made easier by access to inventory information about VoIP entities. The LLDP Inventory TLVs consist of the following:
    - LLDP-MED Hardware Revision TLV allows the device to advertise its hardware revision.
    - LLDP-MED Firmware Revision TLV allows the device to advertise its firmware revision.
    - LLDP-MED Software Revision TLV allows the device to advertise its software revision.
    - LLDP-MED Serial Number TLV allows the device to advertise its serial number.
    - LLDP-MED Manufacturer Name TLV allows the device to advertise the name of its manufacturer.
    - LLDP-MED Model Name TLV allows the device to advertise its model name
    - LLDP-MED Asset ID TLV allows the device to advertise its asset ID

802.1AB MED network policies

You can configure 802.1AB MED network policies to dynamically configure voice VLAN, DSCP, priority, and VLAN tagging on the switch for voice traffic received from an IP phone. When you enable LLDP and configure the MED network policies on the switch, the switch sends the network policies to the IP Phone. The IP phone processes the data in the LLDP PDU and transmits the voice traffic with the appropriate VLAN ID, VLAN tagging, DSCP and priority information.

You can configure MED network policies on a switch port that has ADAC enabled. The network policies that you configure have priority over automatically configured ADAC network policies on a port.

Transmitting LLDPDUs

When a transmit cycle is initiated, the LLDP manager extracts the managed objects from the LLDP local system MIB and formats this information into TLVs. TLVs are inserted into the LLDPDU.

LLDPDU are regularly transmitted at a user-configurable transmit interval (*tx-interval*) or when any of the variables in the LLPDU is modified on the local system (such as system name or management address).

Tx-delay is "the minimum delay between successive LLDP frame transmissions."

TLV system MIBs

The LLDP local system MIB stores the information for constructing the various TLVs to be sent. The LLDP remote systems MIB stores the information received from remote LLDP agents.

LLDPDU and TLV error handling

LLDPDUs and TLVs that contain detectable errors are discarded. TLVs that are not recognized, but that also contain no basic format errors, are assumed to be validated and are stored for possible later retrieval by network management.

802.1AB integration

802.1AB integration provides a set of LLDP TLVs for Avaya IP telephone support.

You can select which Avaya IP phone support TLVs can be transmitted from individual switch ports by enabling or disabling TLV transmit flags for the port. The TLV transmit flags and TLV configuration operate independently of each other. Therefore, you must enable the transmit flag on a switch port for a specific TLV, before the port can transmit that TLV to an Avaya IP phone.

A switch port does not transmit Avaya IP phone support TLVs unless the port detects a connected Avaya IP phone.

PoE conservation level request TLV

With the PoE conservation level request TLV, you can configure the switch to request that an Avaya IP phone, connected to a switch port, operate at a specific power conservation level. The requested conservation level value for the switch can range from 0 to 255, but an Avaya

IP Phone can support only maximum 243 levels. If you request a power conservation level higher the maximum conservation level an Avaya IP Phone can support, the phone reverts to its maximum supported power conservation level. If you select a value of 0 for the PoE conservation level request, the switch does not request a power conservation level for an Avaya IP phone.

If you set the PoE conservation level request TLV on a port and you enable energy-saver for the port, the TLV value is temporarily modified for maximum power savings by the switch. When you disable energy-saver for the port, the switch automatically restores the power conservation level request TLV to the previous value.

If you set the PoE conservation level on a port while AES is active on the port and the maximum PoE Conservation level for the switch is 255, the switch replaces the PoE conservation level stored for AES restoration with the new value you set for the port.

By default, the transmission of PoE conservation level request TLV is enabled on all PoE capable switch ports.

You can only configure the PoE conservation level request TLV on switches that support PoE.

PoE conservation level support TLV

With the PoE conservation level support TLV, an Avaya IP phone transmits information about current power save level, typical power consumption, maximum power consumption, and power conservation level of the IP phone, to a switch port.

Call server TLV

With the call server TLV, you can configure the switch to advertise the IP addresses of a maximum of 8 call servers to connected Avaya IP phones. Avaya IP phones use the IP address information to connect to a call server.

Avaya IP phones use the call server TLV to report which call server it is connected to back to the switch.

The call server TLV supports IPv4 addresses only.

By default, the transmission of the call server TLV is enabled for all ports.

File server TLV

With the file server TLV, you can configure the switch to advertise the IP addresses of a maximum of 4 file servers to connected Avaya IP phones. Avaya IP phones use the IP address information to connect to a file server.

Avaya IP phones use the call server TLV to report which file server it is connected to back to the switch.

The file server TLV supports IPv4 addresses only.

By default, the transmission of the file server TLV is enabled for all ports.

Note:

If your Avaya IP Handset uses SIP, 802.1AB (LLDP) TLVs do not provide all information for the IP Phone. You must specify a fileserver IP address TLV so the IP phone can download the SIP configuration information, because the IP Phone retrieves information related to the SIP domain, port number and transport protocol from the file server.

802.1Q framing TLV

With the 802.1Q framing TLV, you can configure the switch to exchange Layer 2 priority tagging information with Avaya IP phones.

Because the 802.1Q framing TLV operates as an extension of the LLDP Network Policy TLV, you must enable the LLDP MED Capabilities and LLDP MED Network Policy TLVs for the 802.1Q framing TLV to function.

By default, the transmission of the 802.1Q Framing TLV is enabled for all ports.

Phone IP TLV

Avaya IP phones use the phone IP TLV to advertise IP phone IP address configuration information to the switch.

The phone IP TLV supports IPv4 addresses only.

Chapter 6: System configuration using ACLI

The modules in this section provide procedures to configure the switch or stack with ACLI.

Setting user access limitations using ACLI

The administrator can use ACLI to limit user access by creating and maintaining passwords for Web, Telnet, and Console access. This is a two-step process that requires that you first create the password and then enable it.

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

Setting the read-only and read/write passwords

The first step to requiring password authentication when the user logs in to a switch is to edit the password settings. To complete this task, perform the following steps:

1. Access ACLI through the Telnet protocol or a Console connection.
2. From the command prompt, use the **`cli password`** command to change the desired password.

   ```
   cli password {read-only | read-write} <password>
   ```

   Table 10: cli password parameters on page 71 explains the parameters for the **`cli password`** command.

   Table 10: cli password parameters

Parameter	Description
{read-only | read-write}	This parameter specifies if the password change is for read-only access or read/write access.
<password>	If password security is disabled, the length can be 1-15 chars. If password security is enabled, the range for length is 10-15 chars.

3. Press `Enter`.

Enabling and disabling passwords

After you set the read-only and read-write passwords, you can individually enable or disable them for the various switch-access methods. To enable passwords, perform the following task.

1. Access ACLI through the Telnet protocol or a Console connection.
2. From the command prompt, use the **cli password** command to enable the desired password.

   ```
   cli password {telnet | serial} {none | local | radius | tacacs}
   ```

   The following table explains the parameters for the **cli password** command.

   Table 11: cli password parameters

Parameter	Description
{telnet | serial}	Specify whether the password is enabled or disabled for Telnet or the console. Telnet and Web access are connected so that enabling or disabling passwords for one enables or disables passwords for the other.
none | local | radius | tacacs	Specifies the password type to modify: • none: disables the password. • local: uses the locally defined password for serial console or Telnet access. • radius: uses RADIUS authentication for serial console or Telnet access. • tacacs : uses TACACS+ authentication, authorization, and accounting (AAA) services for serial console or Telnet access.

3. Press `Enter`.

Configuring RADIUS authentication

The Remote Authentication Dial-In User Service (RADIUS) protocol is a means to authenticate users through a dedicated network resource. This network resource contains a list of eligible user names and passwords and their associated access rights. When RADIUS is used to authenticate access to a switch, the user supplies a user name and password and this information is checked against the existing list. If the user credentials are valid they can access the switch.

If you select RADIUS Authentication when you set up passwords through ACLI, you must specify the RADIUS server settings to complete the process. Ensure that you enter **Global Configuration** mode in ACLI before you start this task.

To enable RADIUS authentication through ACLI, follow these steps.

1. Access ACLI through the Telnet protocol or a Console connection.
2. From the command prompt, use the **radius-server** command to configure the server settings.

```
radius-server host <address> [secondary-host <address>] port
<num> key <string> [password fallback] timeout
```

Table 12: radius-server parameters on page 73 explains the parameters for the **radius-server** command.

Table 12: radius-server parameters

Parameter	Description
host <address>	The IPv6 or IP address of the RADIUS server that is used for authentication.
[secondary-host <address>]	The secondary-host <address> parameter is optional. If you specify a backup RADIUS server, include this parameter with the IPv6 or IP address of the backup server.
port <num>	The UDP port number the RADIUS server uses to listen for requests.
key <string>	A secret text string that is shared between the switch and the RADIUS server. Enter the secret string, which is a string up to 16 characters in length.
[password fallback]	An optional parameter that enables the password fallback feature on the RADIUS server. This option is disabled by default.
timeout	The RADIUS timeout period.

3. Press `Enter`.

Related RADIUS Commands

When you configure RADIUS authentication, three other ACLI commands are useful to the process:

1. `show radius-server`

   The command has no parameters and displays the current RADIUS server configuration.
2. `no radius-server`

This command has no parameters and clears any previously configured RADIUS server settings.

3. `radius-server password fallback`

   This command has no parameters and enables the password fallback RADIUS option if it you did not set the option when you initially configured the RADIUS server.

Changing switch software in ACLI

Perform the following procedure to change the software version that runs on the switch with ACLI:

Important:
When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

1. Access ACLI through the Telnet protocol or through a Console connection.
2. From the command prompt, use the download command with the following parameters to change the software version:

```
download [address <ipv6_address> | <a.b.c.d>] {image <image
name> | image-if-newer <image name> | diag <image name> |
poe_module_image <image name>} [no-reset] [usb]
```

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

Table 13: download parameters

Parameter	Description
address <ipv6_address> | <a.b.c.d>	The IPv6 or IP address of the TFTP server you use. The address <ipv6_address> | <a.b.c.d> parameter is optional and if you omit it, the switch defaults to the TFTP server specified by the `tftp-server` command unless software download is to occur using a USB Mass Storage Device.
image <image name>	The name of the software image to be downloaded from the TFTP server.
image-if-newer <image name>	This parameter is the name of the software image to be downloaded from the TFTP server if it is newer than the currently running image.
diag <image name>	The name of the diagnostic image to be downloaded from the TFTP server.

Parameter	Description
poe_module_image <image name>	The name of the Power over Ethernet module image to be downloaded from the TFTP server. This option is available only for 4500 Series switches that support Power Over Ethernet.
no-reset	This parameter forces the switch to not reset after the software download is complete.
usb	In the Avaya Ethernet Routing Switch 4500 Series switch, this parameter specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port.
The `image, image-if-newer, diag`, and `poe_module_image` parameters are mutually exclusive; you can execute only one at a time. The address <ip> and usb parameters are mutually exclusive; you can execute only one at a time.	

3. Press `Enter`.

The software download 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. Depending on network conditions, this process can take up to 10 minutes.

When the download is complete, the switch automatically resets unless you used the `no-reset` parameter. The software image initiates a self-test and returns a message when the process is complete. See the following graphic for an example of this message.

Table 14: Software download message output

```
Download Image [/]

Saving Image [-]

Finishing Upgrading Image
```

During the download, the switch is not operational.

You can track the progress of the download by observing the front panel LEDs. For more information about this topic, see LED activity during software download on page 56.

Setting TFTP parameters

Many processes in the switch can use a Trivial File Transfer Protocol (TFTP) server. The following sections describe how to set a default TFTP server for the switch and how to clear these defaults through ACLI:

- Setting a default TFTP server on page 76
- Displaying the default TFTP server on page 76
- Clearing the default TFTP server on page 77

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

Setting a default TFTP server

The switch processes that use a TFTP server often give the switch administrator the option to specify the IP address of a TFTP server to use. Instead of entering this address every time, the switch can store a default IP address.

Specify a default TFTP server for the switch with the **`tftp-server`** command. The syntax of this command is

```
tftp-server [<ipv6_address> | <XXX.XXX.XXX.XXX>]
```

To complete the command, replace either **`ipv6_address`** with the IPv6 address or **`<XXX.XXX.XXX.XXX>`** with the IPv6 or IP address of the default TFTP server. You must run this command in Global Configuration command mode.

Displaying the default TFTP server

You can display the default TFTP server configured for the switch in ACLI at any time by using the **`show tftp-server`** command. This command has no parameters and you run it in Privileged EXEC mode.

Clearing the default TFTP server

You can clear the default TFTP server from the switch and reset it to 0.0.0.0 with the following two commands:

- `no tftp-server`

  This command has no parameters and you run it in Global Configuration command mode.
- `default tftp-server`

  This command has no parameters and you run it in Global Configuration command mode.

Configuration files in ACLI

ACLI provides many options for working with configuration files. Through ACLI, you can display, store, and retrieve configuration files.

For details, see the following sections:

- Displaying the current configuration on page 77
- Storing the current configuration in ASCII file on page 84
- Storing configuration in binary file on page 87
- Restoring configuration from an ASCII file on page 88
- Restoring configuration from a binary file on page 91
- Saving the current configuration on page 92
- Viewing USB files on page 94
- Viewing USB host port information on page 95

Displaying the current configuration

To display the current configuration of switch or a stack, use the **`show running-config`** command, with the following syntax, in Privileged EXEC command mode with no parameters:

The syntax of this command is:

```
show running-config [verbose] [module <value>]
```

You can enter `[module <value>]` parameters individually or in combinations.

Important:

If the switch CPU is busy performing other tasks, the output of the **`show running-config`** command can appear to intermittently stop and start. This is normal operation to ensure that other switch management tasks receive appropriate priority.

Important:

The ASCII configuration generated by the **`show running-config`** command produces a file in which the IP address of the switch is inactive by being commented out using the '!' character. This enables customers to move the configuration between switches without causing issues with duplicate IP addresses.

Variable definitions

The following table defines optional parameters that you can enter after the **`show running-config`** command.

Variable	Value
module <value>	Display configuration of an application for any of the following parameter values: [802.1ab] [aaur] [adac] [arp-inspection] [asset-id] [aur] [banner] [core] [dhcp-relay] [dhcp-snooping] [eap] [energy-saver] [interface] [ip] [ip-source-guard] [ipfix] [ipmgr] [ipv6] [l3] [l3-protocols] [lacp] [logging] [mac-security] [mlt] [nsna] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [ssh] [ssl] [stack] [stkmon] [stp] [vlacp] [vlan]
verbose	Display entire configuration, including defaults and non-defaults.

Job aid: show running-config command output

The following tables show sample output for variations of the **`show running-config`** command.

Table 15: show running-config module mlt command output

```
ERS-4524GT# show running-config module mlt

! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4524GT
! Software version = v5.4.0.057
!
! Displaying only parameters different to default
```

```
!=================================================== enable
configure terminal
!
! *** MLT (Phase 1) ***
!
!
! *** MLT (Phase 2) ***
!
ERS-2500#
```

Table 16: show running-config module ip mlt command output

```
ERS-4524GT# show running-config module ip mlt

! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4524GT
! Software version = v5.4.0.057
!
! Displaying only parameters different to default
!===================================================
enable
configure terminal
!
! *** IP  ***
!
ip default-gateway 172.16.120.1
ip address switch 172.16.120.40
ip address netmask 255.255.255.0
!
! *** MLT (Phase 1) ***
!
!
! *** MLT (Phase 2) ***
!
ERS-2500#
```

Table 17: show running-config command output

```
ERS-4524GT# show running-config


! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4524GT
! Software version = v5.4.0.057
!

! Displaying only parameters different to default
!===================================================
enable

configure terminal
!
```

```
! *** CORE ***
!

! tftp-server 172.16.3.2


!
!
! *** SNMP ***
!

!
snmp-server contact "John Doe"
snmp-server name "ERS-4524GT"
snmp-server

!
! *** IP  ***

!
ip default-gateway 172.16.120.1
ip address switch 172.16.120.39
ip address netmask 255.255.255.0

!
! *** IP Manager ***
!

!
! *** ASSET ID ***

!
!
! *** EAP ***

!
!
! *** IPFIX ***

!
!
! *** System Logging ***

!
!
! *** STACK ***

!
!
! *** Custom Banner ***

!
!
! *** SSH ***
```

```
!
!
! *** SSL ***

!
!
! *** STP (Phase 1) ***

!
!
! *** VLAN ***
!
!
! *** EAP Guest VLAN ***

!
!
! *** EAP Fail Open VLAN ***

!
!
! *** EAP Voip VLAN ***

!
!
! *** Port Mirroring ***

!
!
! *** QOS ***

!
!
! *** RMON ***

!
!
! *** Interface ***

!
!
! *** MLT (Phase 1) ***

!
!
! *** MAC-Based Security ***

!
!
! *** LACP ***

!
!
```

```
! *** ADAC ***

!
!
! *** STP (Phase 2) ***

!
!
! *** VLAN Phase 2***

!
!
! *** IPV6 ***

!
!
! *** MLT (Phase 2) ***

!
!
! *** PoE ***

!
!
! *** Avaya Energy Saver ***

!
!
! *** AUR ***
!
!
! *** AAUR ***

!
!
! *** RTC ***

!
!
! *** L3 ***

!
ip num-routes max-local 3 max-static 13
ip routing
ip route 0.0.0.0 0.0.0.0 172.16.120.1 10

!
!
! *** NSNA ***
!
!
! *** VLACP ***
!
!
```

```
! *** DHCP Relay ***

!
interface vlan 1
ip dhcp-relay min-sec 30
ip dhcp-relay option82-subscriber-id "November"
exit

!
! *** 802.1ab ***
!

!
! *** L3 Protocols ***
!

! --- Proxy ARP ---
! --- UDP Broadcast Forwarding ---

! *** Route Policies ***


!
!
! *** OSPF ***
!
!
! *** RIP ***

!
! *** DHCP SNOOPING ***
!
ip dhcp-snooping
ip dhcp-snooping option82
ip dhcp-snooping vlan 1
ip dhcp-snooping vlan 1 option82
interface FastEthernet ALL
ip dhcp-snooping port 1 trusted exit
ip dhcp-relay option82-subscriber-id "December" exit
!
! *** ARP INSPECTION ***
!
!
! *** IP SOURCE GUARD ***
!
!
! *** STACK MONITOR ***
!
ERS-2500#
```

Storing the current configuration in ASCII file

For all switches in the Avaya Ethernet Routing Switch 4500 Series, you can store the configuration file to a TFTP server and a USB Mass Storage Device through the front panel USB drive. You can store the current configuration into ASCII file type. You can use the following commands to store the configuration in an ASCII file:

- copy running-config tftp command on page 84
- copy running-config usb command on page 85
- script command on page 85

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

copy running-config tftp command

To copy contents of the current configuration file to another file on the TFTP server, use the following command in Privileged EXEC command mode.

```
copy running-config tftp [address <A.B.C.D>] [filename <WORD>]
[module <value>] [verbose]
```

You can enter `[module <value>]` parameters individually or in combinations.

You can also execute this command in the Global Configuration command mode.

Variable definitions

The following table defines the parameters that you enter with the **`copy running-config tftp [address <A.B.C.D>] [filename <WORD>] [module <value>] [verbose]`** command.

Variable	Value
address <A.B.C.D>	Specifies the IP address of the TFTP server.
filename <WORD>	Specifies the filename to store configuration commands on the TFTP server.
module <value>	Display configuration of an application for any of the following parameter values: [802.1ab] [aaur] [adac] [arp-inspection] [asset-id] [aur] [banner] [core] [dhcp-relay] [dhcp-snooping] [eap] [energy-saver] [interface] [ip] [ip-source-guard] [ipfix] [ipmgr] [ipv6] [l3] [l3-protocols] [lacp] [logging] [mac-security] [mlt] [nsna] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [ssh] [ssl] [stack] [stkmon] [stp] [vlacp] [vlan]

Variable	Value
verbose	Copies the entire configuration, including defaults and non-defaults.

Important:
Use the **`copy running-config tftp`** command only from the base unit in a stack.

copy running-config usb command

To copy the contents of the current configuration file to a USB storage device, use the following command in Privileged EXEC command mode.

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

You can enter `[module <value>]` parameters individually or in combinations.

You can also execute this command in the Global Configuration command mode.

Variable definitions

The following table defines the parameters that you enter with the **`copy running-config usb [filename <WORD>] [module <value>] [verbose]`** command.

Variable	Value
filename <WORD>	Specifies the filename to store configuration commands on the TFTP server.
module <value>	Display configuration of an application for any of the following parameter values: [802.1ab] [aaur] [adac] [arp-inspection] [asset-id] [aur] [banner] [core] [dhcp-relay] [dhcp-snooping] [eap] [energy-saver] [interface] [ip] [ip-source-guard] [ipfix] [ipmgr] [ipv6] [l3] [l3-protocols] [lacp] [logging] [mac-security] [mlt] [nsna] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [ssh] [ssl] [stack] [stkmon] [stp] [vlacp] [vlan]
verbose	Copies the entire configuration, including defaults and non-defaults.

script command

Use the **`script`** command to create an entry (either a TFTP or an USB entry) in the ASCII configuration script table.

Important:
When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

The syntax for the **script** command is:

```
script <1-127> {bootp | load-on-boot <1-127> | tftp <hostname | IP>
<filename>| usb [unit<1-8>] <filename>}
```

The **script** command is executed in the Global Configuration command mode.

Table 18: script parameters on page 86 outlines the parameters for this command.

Table 18: script parameters

Parameters	Description
<1-127>	The index of the entry to be used.
usb	Creates an USB entry.
<1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack.
tftp	Creates a TFTP entry.
<hostname | ip>	The hostname or IP address of the TFTP server.
filename	The name of the file to be saved.
bootp	Indicates script from the TFTP server, filename, and IP address obtained using BOOTP
load-on-boot	Specifies the load-on-boot priority. Values range from 1 to 127. If you omit this parameter, the entry is created or modified for manual upload and downloads only.

Use the **script upload** command to save the contents of the current configuration. The syntax for the **script upload** is:

```
script upload <1-127>
```

The **script upload** command is executed in the Privileged EXEC command mode.

Table 19: script upload parameters on page 86 outlines the parameters for this command.

Table 19: script upload parameters

Parameters	Description
<1-127>	The index of the entry to be used and must correspond with the index used to create an entry.

show script status command

Use the **show script status** command to view the status of one or all the entries. The syntax for the **show script status** command is:

```
show script status [<1-127>]
```

The **show script status** command is executed in the Privileged EXEC command mode.

Table 20: show script status parameters on page 87 outlines the parameters for this command.

Table 20: show script status parameters

Parameters	Description
<1-127>	The index of the entry to be used.

Storing configuration in binary file

For all switches in the Avaya Ethernet Routing Switch 4500 Series, you can store the configuration file to a TFTP server and a USB Mass Storage Device through the front panel USB drive. You can store the current configuration into binary configuration file types. You can store the configuration in binary files using the **copy config {tftp | usb}** command. For more information, see the following sections:

- copy config tftp command on page 87
- copy config usb command on page 88

copy config tftp command

Use the **copy config tftp** command to store configuration in a binary file to a TFTP server. The syntax for the **copy config tftp** command is:

```
copy config tftp {address <A.B.C.D>| filename <filename>}
```

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address.

The **copy config tftp** command is executed in the Privileged EXEC command mode.

The following table outlines the parameters for the **copy config tftp** command.

Table 21: copy config tftp command parameters

Parameters	Description
Address	The IP address of the TFTP server.
<filename>	The name of the file to be retrieved.

copy config usb command

Use the **`copy config usb`** command to store a configuration file to a USB Mass Storage Device. The syntax for the **`copy config usb`** command is:

```
copy config usb {filename <filename> | unit <1-8>
```

The **`copy config usb`** command is executed in the Privileged EXEC command mode.

Table 22: copy config usb command parameters on page 88 outlines the parameters for the **`copy config usb`** command.

Table 22: copy config usb command parameters

Parameters	Description
<filename>	The name of the file to be retrieved.
<1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack .

Restoring configuration from an ASCII file

You can restore the configuration from an ASCII file using the following commands:

- configure { network | usb } command on page 88
- script command on page 89

configure { network | usb } command

Use the **`configure {network | usb}`** command to restore contents of the current configuration from an ASCII file. The syntax for the **`configure {network | usb}`** is:

```
configure {network [address <A.B.C.D>] filename <filename>| usb
filename <filename> [unit <1-8>]}
```

The **`configure {network | usb}`** command is executed in the Privileged EXEC command mode.

Table 23: Config {network | usb} command parameters on page 89 outlines the parameters for this command.

Table 23: Config {network | usb} command parameters

Parameter	Description
network	Retrieve the configuration from a TFTP server.
<A.B.C.D>	The IP address of the TFTP server.
usb	Retrieve the configuration from an USB mass storage device.
<1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack.
<filename>	The name of the file to be retrieved.

script command

Use the **script** command to restore an entry (either a TFTP or an USB entry) in the ASCII configuration script table.

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

The syntax for the **script** command is:

```
script <1-127> {usb [unit<1-8>] <filename> | tftp <hostname | IP>
<filename>}
```

The **script** command is executed in the Privileged EXEC command mode.

Table 24: script parameters

Parameters	Description
<1-127>	The index of the entry to be restored.
usb	Restores an USB entry.
<1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack.
tftp	Restores a TFTP entry.
<hostname | ip>	The hostname or IP address of the TFTP server.
filename	The name of the file to be restored.

show script status command

Use the **show script status** command to view the status of one or all the entries. The syntax for the **show script status** command is:

```
show script status [<1-127>]
```

The **show script status** command is executed in the Privileged EXEC command mode.

Note:

By default, a script table index is present as a bootp entry. If a bootp server is connected to the stack or switch, you can automatically configure the switch using an ASCII file present on the bootp server.

The following is an example output for **show script** command:

```
4526T-PWR(config)#show script 2
Table index: 2
Load script on boot: Yes
Boot priority: 1
Script source: bootp://
```

Table 25: show script status parameters

Parameters	Description
<1-127>	The index of the entry to be used.

script run command

Use the **script run** command to load the script from an ASCII file to a tftp server or USB Mass Storage Device.

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

The syntax for the **script run** command is:

```
script run { <1-127> | tftp <A.B.C.D> <filename> | usb [unit <1-8>
<filename>] }
```

The **`script run`** command is executed in the Privileged EXEC command mode.

Table 26: script run command parameters on page 91 outlines the parameters for this command.

Table 26: script run command parameters

Parameters	Description
<1-127>	The index of the ASCII configuration script table entry to be used.
<A.B.C.D>	The IP address of the tftp server to load the script.
<filename>	The name of the file to be restored.
<1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack.

Restoring configuration from a binary file

You can restore the configuration from a binary file using the following commands:

- copy tftp config command on page 91
- copy usb config command on page 92

copy tftp config command

Use the **`copy tftp config`** to restore a configuration from a binary file from a TFTP server. You can also use this command to copy the configuration of a switch in a stack to a stand-alone switch and to replace units in the stack.

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address.

The syntax for the **`copy tftp config`** file is:

```
copy tftp config address <XXX.XXX.XXX.XXX> filename <name> unit <unit
number>
```

The **`copy tftp config`** command is executed in Privileged EXEC command mode.

Table 27: copy tftp config parameters on page 92 outlines the parameters for this command.

Table 27: copy tftp config parameters

Parameter	Description
address <XXX.XXX.XXX.XXX>	The IP address of the TFTP server.
filename <name>	The name of the file to be retrieved.
unit <unit number>	The number of the stack unit.

copy usb config command

Use the **`copy usb config`** command to restore a configuration file from a USB Mass Storage Device. The syntax for the **`copy usb config`** command is:

```
copy usb config filename <name>
```

The **`copy usb config`** command is executed in the Privileged EXEC command mode. The only parameter for this command is the name of the file to be retrieved from the USB device.

Saving the current configuration

The configuration currently in use on a switch is regularly saved to the flash memory automatically. However, you can manually initiate this process using the **`copy config nvram`** command. This command takes no parameters and you must run it in Privileged EXEC mode. If you have disabled the AutosaveToNvramEnabled function by removing the default check in the AutosaveToNvRamEnabled field, the configuration is not automatically saved to the flash memory.

write memory command

The **`write memory`** command copies the current configuration to NVRAM. The syntax for the **`write memory`** command is:

```
write memory
```

The **`write memory`** command is in the exec command mode.

The **`write memory`** command has no parameters or variables.

save config command

The **`save config`** command copies the current configuration to NVRAM. The syntax for the **`save config`** command is:

```
save config
```

The **`save config`** command is in the exec command mode.

The **`save config`** command has no parameters or variables.

Automatically downloading a configuration file

Enable this feature through ACLI by using the **`configure network`** and **`script load-on-boot`** command. Use these commands to immediately load and run a script and to configure parameters to automatically download a configuration file when the switch or stack is booted.

> **Important:**
> When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

The syntax for the **`configure network`** command is

```
configure network load-on-boot {disable | use-bootp | use-config}
address <XXX.XXX.XXX.XXX> filename <name>
```

Table 28: configure network parameters on page 93 outlines the parameters for this command.

Table 28: configure network parameters

Parameter	Description
load-on-boot {disable | use-bootp | use-config}	The settings to automatically load a configuration file when the system boots: • **disable:** disable the automatic loading of config file • **use-bootp:** load the ASCII configuration file at boot and use BootP to obtain values for the TFTP address and file name • **use-config:** load the ASCII configuration file at boot and use the locally configured values for the TFTP address and file name **Important:** If you omit this parameter, the system immediately downloads and runs the ASCII configuration file.
address <XXX.XXX.XXX.XXX>	The IP address of the TFTP server.
filename <name>	The name of the configuration file to use in this process

You must run this command in the Privileged EXEC mode.

You can view the current switch settings for this process using the **`show config-network`** command. This command takes no parameters.

The syntax for the **`script load-on-boot`** command is

```
script <1-127> load-on-boot <1-127> [usb [unit <1-8>] <filename> |
tftp <A.B.C.D> <filename> | bootp]
```

Table 29: script load-on-boot parameters on page 94 outlines the parameters for this command.

Table 29: script load-on-boot parameters

Parameter	Description
script <1-127>	The index of the ASCII configuration script table entry to be used.
load-on-boot <1-127>	The boot priority of the ASCII configuration script table entry.
[usb | tftp | bootp]	The settings to automatically load a configuration file when the system boots: • **usb:** load the configuration file at boot from an USB mass storage device • **tftp:** load the ASCII configuration file at boot from a TFTP server • **bootp:** load the ASCII configuration file at boot and use BootP to obtain values for the TFTP address and file name
unit <1-8>	The number of the unit in which the USB mass storage device is inserted in.
<filename>	The name of the configuration file to use in this process.
<A.B.C.D>	The IP address of the TFTP server.

You must run this command in the global configuration mode.

You can view the current switch settings for this process using the `show script [status] <1-127>` command.

Viewing USB files

Use the following procedure to view the USB files. You can display configuration files stored on a USB device in a unit in a stack.

Prerequisites

Log on to the User EXEC mode in ACLI.

Procedure steps

Enter the following command:

```
show usb-files [dir <WORD> | tree | unit <1-8>
```

Table 30: show usb-files parameters

Parameter	Description
dir <WORD>	Specifies a directory in which to locate USB files to display.
tree	Specifies subdirectories. .
unit <1-8>	The number of the switch unit within a stack.

Job aid

Following is an output example for the show usb-files command:

```
ERS4500#show usb-files
USB file list - Stand-alone
Listing Directory USB_BULK:
657 Feb 17 2009 IP.CFG
6217432 Mar 3 2009 4500_53044.img
1589514 Feb 25 2009 4500_5303.bin
2048 Mar 4 2009 ABC/
```

Viewing USB host port information

Use this procedure to view USB host port information. You can display the USB host port information for a unit in a stack.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Enter the following command:

```
show usb-host-port [unit <1-8>]
```

Table 31: show usb-host-port parameters

Variable	Description
unit <1-8>	Specifies a specific switch unit within a stack. Values range from 1 to 8.

Setting up a terminal

You can customize switch terminal settings to suit the preferences of a switch administrator. You must perform this operation in the Command Line Interface.

The **`terminal`** command configures terminal settings. These settings include terminal length and terminal width.

The syntax of the **`terminal`** command is:

```
terminal length <0-132> width <1-132>
```

Run the terminal command in User EXEC command mode. The following table describes the for the terminal command.

Table 32: terminal parameters

Variable	Description
length	Set the length of the terminal display in lines; the default is 23. **Important:** If you set the terminal length to 0, the pagination is disabled and the display scrolls continuously.
width	Set the width of the terminal display in characters; the default is 79.

You can use the `show terminal` command at any time to display the current terminal settings. This command takes no parameters and you must run it in the EXEC command mode.

Setting Telnet access

You can access ACLI through a Telnet session. To access ACLI remotely, the management port must have an assigned IP address and remote access must be enabled.

Important:

Multiple users can simultaneously access ACLI system through the serial port, a Telnet session, and modems. The maximum number of simultaneous users is 4, plus 1 each at the serial port for a total of 12 users on the stack. All users can configure the switch simultaneously.

For details about viewing and changing the Telnet-allowed IP addresses and settings, see the following sections:

- telnet-access command on page 97
- no telnet-access command on page 98
- default telnet-access command on page 99

telnet-access command

The **telnet-access** command configures the Telnet connection that you use to manage the switch. Run the telnet-access command through the console serial connection.

The syntax for the **telnet-access** command is:

```
telnet-access [enable | disable] [login-timeout <1-10>] [retry
<1-100>] [inactive-timeout <0-60>] [logging {none | access | failures
| all}] [source-ip <1-50> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]
```

Run the **telnet-access** command in Global Configuration command mode.

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

Table 33: telnet-access parameters

Parameters	Description
enable | disable	Enable or disable Telnet connection.
login-timeout <1-10>	Specify in minutes the time for the Telnet connection to be established after the user connects to the switch. Enter an integer from 1–10.

Parameters	Description
retry <1-100>	Specify the number of times the user can enter an incorrect password before the connection closes. Enter an integer from 1–100.
inactive-timeout <0-60>	Specify in minutes the duration before an inactive session terminates.
logging {none | access | failures | all}	Specify the events for which you want to store details 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.
[source-ip <1-50> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]	Specify the source IP address from which connections can occur. Enter the IP address in dotted-decimal notation. Mask specifies the subnet mask from which connections can occur; enter IP mask in dotted-decimal notation.

no telnet-access command

The **no telnet-access** command disables the Telnet connection. The **no telnet-access** command is accessed through the console serial connection.

The syntax for the **no telnet-access** command is:

```
no telnet-access [source-ip [<1-50>]]
```

Run the **no telnet-access** command in Global Configuration command mode.

The following table describes the variables for the **no telnet-access** command.

Table 34: no telnet-access parameters

Variables	Description
source-ip [<1-50>]	Disable the Telnet access. When you do not use the optional parameter, the source-ip list is cleared, which means the first index is 0.0.0.0./0.0.0.0. and the second to fiftieth indexes are 255.255.255.255/255.255.255.255. When you specify a source-ip address, the specified pair is 255.255.255.255/255.255.255.255.

Variables	Description
	Important: These same source IP addresses are in the IP Manager list. For more information about the IP Manager list, see Chapter 3.

default telnet-access command

The **default telnet-access** command sets the Telnet settings to the default values.

The syntax for the **default telnet-access** command is

```
default telnet-access
```

Run the **default telnet-access** command in Global Configuration command mode.

Setting boot parameters using ACLI

The command described in this section is used to boot the switch or stack and to set boot parameters.

boot command

The **boot** command performs a soft-boot of the switch or stack.

The syntax for the **boot** command is

```
boot [default] [unit <unit no>]
```

Run the **boot** command in Privileged EXEC command mode.

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

Table 35: boot parameters

Variables	Description
default	Restore switch or stack to factory-default settings after rebooting.
unit <unit no>	Specify which unit of the stack is rebooted. This command is available only in stack mode. Enter the unit number of the switch you want to reboot.

Important:
When you reset to factory defaults, the switch or stack retains the stack operational mode, the last reset count, and the reason for the last reset; these three parameters are not reset to factory defaults.

Viewing the agent and image software load status using ACLI

The command described in this section is used to display the currently loaded and operational software status for agent and image loads, either individually or combined, for an individual switch or a stack.

show boot command

The **`show boot`** command displays the currently loaded and operational software load status.

The syntax for the **`show boot`** command is

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

Run the **`show boot`** command in User EXEC command mode.

Variable definitions

The following table describes the optional parameters you can enter with the **`show boot [diag] [image]`** command.

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

Important:
When the currently loaded and operational software status is displayed for a stack, the unit number is replaced by the word **All**.

Job aid: show boot command output

The following figures show sample individual switch output for variations of the **`show boot [diag] [image]`** command.

```
ERS-4524GT>show boot
Unit  Agent Image Active Image Diag Image Active Diag
----- ----------- ------------ ---------- -----------
1     5.4.0.065   5.4.0.065    5.3.0.0    5.3.0.0
* - Unit requires reboot for new Active Image to be made operational.
# - Unit requires reboot for new Diag to be made operational.
ERS-4524GT>
```

Figure 10: show boot command output

```
ERS-4524GT>show boot diag
Unit  Diag Image Active Diag
----- ---------- -----------
1     5.3.0.0    5.3.0.0
# - Unit requires reboot for new Diag to be made operational.
ERS-4524GT>
```

Figure 11: show boot diag command output

```
ERS-4524GT>show boot image
Unit  Agent Image Active Image
----- ----------- ------------
1     5.4.0.065   5.4.0.065
* - Unit requires reboot for new Active Image to be made operational.
ERS-4524GT>
```

Figure 12: show boot image command output

Defaulting to BootP-when-needed

The BootP default value is BootP-when-needed. The switch can boot and the system can automatically seek a BootP server for the IP address.

If the device has an assigned IP address and the BootP process times out, the BootP mode remains in the default mode BootP-when-needed.

However, if the device has no assigned IP address and the BootP process times out, the BootP mode automatically changes to BootP disabled. This change to BootP disabled is not stored, and the BootP reverts to the default value of BootP-when-needed after the device reboots.

When you upgrade the system, the switch retains the previous BootP value. When the switch resets to default after an upgrade, the system moves to the default value of BootP-when-needed.

Configuring with the command line interface

This section covers ACLI commands needed to configure BootP parameters:

- ip bootp server command on page 102
- no ip bootp server command on page 102
- default ip bootp server command on page 103

ip bootp server command

The **`ip bootp server`** command configures BootP on the current instance of the switch or server. Use this command to change the value of BootP from the default value, which is BootP-when-needed.

The syntax for the **`ip bootp server`** command is:

```
ip bootp server {always | disable | last | needed}
```

Run the **`ip bootp server`** command in Global Configuration command mode.

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

Table 36: ip bootp server parameters

Parameters and variables	Description
always | disable | last I needed	Specify when to use BootP: • always: Always use BootP. • disable: Never use BootP. • last: Use BootP or the last known address. • needed: Use BootP only when needed. **Important:** The default value is to use BootP when needed.

no ip bootp server command

The **`no ip bootp server`** command disables the BootP/DHCP server.

The syntax for the **`no ip bootp server`** command is

```
no ip bootp server
```

Run the **no ip bootp server** command in Global Configuration command mode.

default ip bootp server command

The default **ip bootp server** command uses BootP when needed.

The syntax for the **default ip bootp server** command is:

```
default ip bootp server
```

Run the **default ip bootp server** command in Global Configuration command mode.

Customizing ACLI banner

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

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 ACLI banner using ACLI, see the following commands:

- show banner command on page 103
- banner command on page 104
- no banner command on page 104

show banner command

The **show banner** command displays the banner.

The syntax for the **show banner** command is:

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

Run the **show banner** command in Privileged EXEC command mode.

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

Table 37: show banner parameters

Parameters and variables	Description
static | custom	Specify which banner is currently set to be displayed:

Parameters and variables	Description
	• static • custom

banner command

The **banner** command specifies the banner that is displayed at startup; either static or custom.

The syntax for the **banner command** is:

```
banner {static | custom} <line number> "<LINE>"<disabled>
```

The following table describes the parameters for this command.

Table 38: banner parameters

Parameters and variables	Description
static | custom	Set the display banner as • static • custom
line number	Enter the banner line number you are setting. The range is 1–19.
LINE	Specify the characters in the line number.
disabled	Disable the banner display.

Run the **banner** command in Global Configuration command mode.

no banner command

The **no banner** command clears all lines of a previously stored custom banner. This command sets the banner type to the default setting (STATIC).

The syntax for the **no banner** command is

```
no banner
```

Run the **no banner command** in Global Configuration command mode.

ACLI Help

To obtain help on the navigation and use of the Command Line Interface (ACLI), use the following command:

```
help {commands | modes}
```

Use **`help commands`** to obtain information about the commands available in ACLI organized by command mode. A short explanation of each command is also included.

Use **`help modes`** to obtain information about the command modes available and ACLI commands used to access them.

These commands are available in any command mode.

Configuring AUR

This section describes ACLI commands used in AUR configuration.

show stack auto-unit-replacement command

The **`show stack auto-unit-replacement`** command displays the current AUR settings.

The syntax for this command is

```
show stack auto-unit-replacement
```

The **`show stack auto-unit replacement`** command is in all command modes.

No parameters or variables are available for the **`show stack auto-unit replacement`** command.

stack auto-unit-replacement enable command

The **`stack auto-unit-replacement enable`** command enables AUR on the switch.

The syntax for this command is

```
stack auto-unit-replacement enable
```

Run the **stack auto-unit-replacement enable** command in Global Configuration mode.

No parameters or variables are available for the **stack auto-unit-replacement enable** command.

no stack auto-unit-replacement enable command

The **no stack auto-unit-replacement enable** command disables AUR on the switch.

The syntax for this command is

```
no stack auto-unit-replacement enable
```

Run the **no stack auto-unit-replacement enable** command in Global Configuration mode.

No parameters or variables are available for the **no stack auto-unit-replacement enable** command.

default stack auto-unit-replacement enable command

The **default stack auto-unit-replacement enable** command restores the default AUR settings.

The syntax for this command is

```
default stack auto-unit-replacement enable
```

Run the **default stack auto-unit-replacement enable** command in Global Configuration mode.

No parameters or variables are available for the **default stack auto-unit-replacement enable** command.

stack auto-unit-replacement config save enable

The **stack auto-unit-replacement config save enable** command enables automatic configuration saves for non-base units.

No parameters or variables are available for the **stack auto-unit-replacement config save enable** command.

1. Enter Global Configuration mode.
2. Enter `stack auto-unit-replacement config save enable`.
3. Press `Enter`.

stack auto-unit-replacement config save disable

The **`stack auto-unit-replacement config save disable`** command disables automatic configuration saves for non-base units.

No parameters or variables are available for the **`stack auto-unit-replacement config save disable`** command.

1. Enter Global Configuration mode.
2. Enter `stack auto-unit-replacement config save disable`.
3. Press `Enter`.

stack auto-unit-replacement config restore unit

The **`stack auto-unit-replacement config restore unit <1-8>`** command restores the saved configuration to a non-base unit. Use the base unit console in Privileged Mode to enter this command.

1. Enter Privileged Mode.
2. Enter `stack auto-unit-replacement config restore unit` with the unit number <1-8> to restore.
3. Press `Enter`.

stack auto-unit-replacement config save unit

The **`stack auto-unit-replacement config save unit <1-8>`** command saves the configuration of the selected non-base unit to the base unit, regardless of the state of the AUR feature. Use the base unit console in Privileged Mode to enter this command.

1. Enter Privileged Mode.
2. Enter `stack auto-unit-replacement config save unit` with the unit number <1-8> to save.
3. Press `Enter`.

Agent Auto Unit Replacement

Use ACLI commands in the following sections to manage and configure AAUR. You can currently manage this functionality only through ACLI.

stack auto-unit-replacement-image enable command

Use the **`stack auto-unit-replacement-image enable`** command to enable AAUR. Because AAUR is enabled by default, use this command only if this functionality was previously disabled.

The syntax for this command is

```
stack auto-unit-replacement-image enable
```

Run the **`stack auto-unit-replacement-image enable`** command in Global Configuration command mode.

no stack auto-unit-replacement-image-enable command

Use the **`no stack auto-unit-replacement-image enable`** command to disable AAUR. Because AAUR is enabled by default, you must run this command if you do not want AAUR functionality on a switch.

The syntax for this command is

```
no stack auto-unit-replacement-image enable
```

The **`no stack auto-unit-replacement-image enable`** command is executed in the Global Configuration command mode.

default stack auto-unit-replacement-image enable command

Use the **`default stack auto-unit-replacement-image enable`** command to set the AAUR functionality to the factory default of enabled.

The syntax of this command is

```
default stack auto-unit-replacement-image enable
```

Run the **`default stack auto-unit-replacement-image enable`** command in Global Configuration command mode.

show stack auto-unit-replacement-image command

Use the **show stack auto-unit-replacement-image** command to view the current status of the AAUR functionality.

The syntax of this command is

`show stack auto-unit-replacement-image`

Run the **show stack auto-unit-replacement-image command** in User EXEC command mode.

Configuring DAUR

There are no commands to separately enable or disable DAUR.

Setting Stack Forced Mode

This section describes the procedures and commands to configure Stack Forced Mode on a two unit stack.

Use ACLI Global Configuration command mode to configure Stack Forced Mode.

This section contains the procedures to configure **stack forced-mode**.

Configuring stack forced-mode

Use the following procedure to configure **stack forced-mode**:

1. Enter `<no | default | show> stack forced-mode`.
2. Press `Enter`.

Job aid

The following table defines the options for the **stack forced-mode** command.

Table 39: Options for stack forced-mode

Option	Definition
<>	Enable Stack Forced Mode.

no	Disable Stack Forced Mode.
default	Return to the default setting for Stack Forced Mode.
show	Show Stack Forced Mode status for the switch. The following list shows the possible responses: • `Forced-Stack Mode: Enabled Device is not currently running in forced Stack Mode.` • `Forced-Stack Mode: Enabled Device is currently running in forced Stack Mode.` • `Forced-Stack Mode: Disabled Device is not currently running in forced Stack Mode.`

Displaying complete GBIC information

You can obtain complete information for a GBIC port using the following command:

```
show interfaces gbic-info <port-list>
```

Substitute **`<port-list>`** with the GBIC ports for which to display information. If no GBIC is detected, this command shows no information.

This command is available in all command modes.

Displaying hardware information

To display a complete listing of information about the status of switch hardware in ACLI, use the following command:

```
show system [verbose]
```

The **`[verbose]`** option displays additional information about fan status, power status, and switch serial number.

Switch hardware information is displayed in a variety of locations in EDM. You need no special options in these interfaces to display the additional information.

Shutdown command

The switch administrator can use this feature to safely shut down the switch without interrupting a process or corrupting the software image.

After you issue the command, the configuration is saved and blocking is performed, and the user is notified that it is safe to power off the switch.

The syntax for the **shutdown** command is

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

Substitute `<minutes-to-wait>` with the number of minutes to wait for user intervention before the switch resets. If this parameter is not specified, the switch waits for 10 minutes before resetting.

Use the shutdown command to safely shut down and power off the switch. After you initiate the shutdown command, the switch saves the current configuration which allows users to power off the switch within the specified time period (1 to 60 minutes); otherwise, the switch performs a reset.

When you initiate the shutdown command in ACLI, the following message appears: `Shutdown (y/n) ?`

Enter `yes` at this prompt to shut down the switch.

The following warning message appears:

```
Warning the switch/stack has been set to reboot in <xx> minutes. Current
configuration has been saved, no further configuration changes can be saved until
reboot occurs or 'shutdown cancel' command is issued.
```

The syntax for the shutdown command is

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

After you initiate the shutdown command, all existing and subsequent sessions display the following message:

```
Stack will reset in <xxxx> seconds.
```

While existing ACLI sessions do not receive a warning message, all subsequent ACLI sessions display the following message:

```
The shutdown process is in progress. It is safe to poweroff the stack. Configuration
changes will not be saved. Shutdown has blocked the flash. Autoreset in <xxxx>
seconds.
```

EDM does not receive any shutdown warning messages.

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

Table 40: Shutdown command variables

Variables	Description
force	Instruct the switch to skip the shutdown confirmation prompt.
minutes-to-wait <1-60>	Specify the number of minutes that pass before the switch resets itself The default wait time is 10 minutes.
cancel	Cancel all scheduled switch shutdowns.

Important:

Any configurations or logins performed on the switch after you initiate the shutdown command are not saved to NVRAM and are lost after the reset.

Run the **`shutdown`** command in **privExec** command mode.

Reload command

The **`reload`** ACLI command provides you with a configuration rollback mechanism to prevent loss of connectivity to a switch, typically for remote configurations.

Use the **`reload`** command to temporarily disable the autosave feature for a specified time period, so you can make configuration changes on remote switches without affecting the currently saved configuration.

During the interval in which the autosave feature is disabled by the **`reload`** command, you must use the **`copy config nvram`** command to manually save your configurations.

Initiate the **`reload`** command before you start the switch configuration commands. After you initiate the command in ACLI, the following message appears:

```
Reload (y/n) ?
```

Enter `yes` at this prompt to set the switch reload.

The following warning message appears:

```
Warning the switch/stack has been set to reload in <xx> minutes.
Current configuration has NOT been saved. Configuration must be
explicitly saved.
```

After the reload timer expires, the switch resets, reloads the last saved configuration, and re-enables the autosave feature.

The syntax for the **`reload`** command is

```
reload [force] [minutes-to-wait] [cancel]
```

The following table describes the variables for the **`reload`** command.

Table 41: Reload command variables

Variables	Description
force	Instruct the switch to skip the reload confirmation prompt.
minutes-to-wait	Specify the number of minutes that pass before the switch resets itself. The default wait time is 10 minutes.
cancel	Cancel all scheduled switch reloads.

To abort the switch reload before the timer expires, you must enter the `reload cancel` command.

The **`reload`** command provides you with a safeguard against any misconfigurations when you perform dynamic configuration changes on a remote switch.

The following example describes how you can use the **`reload`** command to prevent connectivity loss to a remote switch:

- Enter ACLI command `reload force minutes-to-wait 30`. This instructs the switch to reboot in 30 minutes and load the configuration from NVRAM. During the 30-minute period, autosave of the configuration to NVRAM is disabled.
- Execute dynamic switch configuration commands, which take effect immediately. These configurations are not saved to NVRAM.
- If the configurations cause no problems and switch connectivity is maintained, you can perform one of the following tasks:
- Save the current running configuration using the **`copy config nvram`**, command.
- Cancel the reload using the **`reload cancel`** command.

If you make an error while executing the dynamic switch configuration commands that results in loss of switch connectivity (for example, if you make an error in the IP address mask, in the Multi-Link Trunking configuration, or in VLAN trunking), the **`reload`** command provides you with a safeguard. When the reload timer expires, the switch reboots to the last saved configuration, and connectivity is re-established. Consequently, you need not travel to the remote site to reconfigure the switch.

restore factory-default command

The **`restore factory-default`** command resets both switch and stack NVRAM blocks to the default configuration. The first NVRAM block will be active after the switch and stack resets.

The syntax for the **`restore factory-default`** command is:

```
restore factory-default [-y]
```

the [-y] parameter instructs the switch not to prompt for confirmation.

Configuring IPv6

Use the following procedures to configure IPv6:

- Enabling IPv6 interface on the management VLAN on page 114
- Configuring IPv6 interface on the management VLAN on page 115
- Displaying the IPv6 interface information on page 115
- Displaying IPv6 interface addresses on page 116
- Configuring an IPv6 address for a switch or stack on page 117
- Displaying the IPv6 address for a switch or stack on page 118
- Configuring IPv6 interface properties on page 118
- Disabling IPv6 interface on page 120
- Displaying the global IPv6 configuration on page 120
- Configuring an IPv6 default gateway for the switch or stack on page 121
- Displaying the IPv6 default gateway on page 121
- Configuring the IPv6 neighbor cache on page 121
- Displaying the IPv6 neighbor information on page 122
- Displaying IPv6 interface ICMP statistics on page 122
- Displaying IPv6 interface statistics on page 123
- Displaying IPv6 TCP statistics on page 124
- Displaying IPv6 TCP listeners on page 125
- Displaying IPv6 UDP statistics and endpoints on page 125

You can only execute ACLI commands for IPv6 interface configuration on the base unit of a stack. Use the Global Configuration mode to execute IPv6 commands.

Enabling IPv6 interface on the management VLAN

Use the following procedure to enable an IPv6 interface to the management VLAN:

ipv6 interface enable

1. At the config prompt, enter `interface vlan 1`.
2. Enter `ipv6 interface enable`.
3. Enter `exit` to return to the main menu.

Use the following procedure to enable ipv6 admin status:

ipv6 enable

Enter `ipv6 enable`.

Job aid

The following table lists the variables and definitions for **`ipv6 enable`**:

Table 42: IPv6 variables and definitions

Variable	Definition
enable	Default admin status: disable

Configuring IPv6 interface on the management VLAN

Use the following procedures to assign an IPv6 address to a VLAN:

config vlan

1. Go to the `config` prompt in ACLI.
2. Enter `interface vlan 1`.
3. Enter `ipv6 interface enable`.
4. Enter `exit` to return to the main menu.

Displaying the IPv6 interface information

Use the following procedure to display the IPv6 interface information:

show ipv6 interface

Enter `show ipv6 interface`.

Job aid

The following graphic shows the results of the **`show ipv6 interface`** command.

```
4526(config)# show ipv6 interface
==========================================================================================
                                     Interface Information
==========================================================================================
IFINDX  VLAND  MTU   PHYSICAL        ADMIN    OPER    RCHBLE   RETRAN   TYPE
        -ID          ADDRESS         STATE    STATE   TIME     TIME
------------------------------------------------------------------------------------------
10001   1      1522  0:11:f9:34:88:0 enabled  up      30000    1000     ETHER
==========================================================================================
                                     Address Information
==========================================================================================
INTF    IPV6                                  TYPE     ORIGIN   STATUS
INDEX   ADDRESS
------------------------------------------------------------------------------------------
10001   3000:0:0:0:0:0:0:99                   UNICAST  MANUAL   PREFERRED
10001   fe80:0:0:0:211:f9ff:fe34:8800         UNICAST  OTHER    UNKNOWN

1 out of 1 Total Num of Interface Entries displayed
2 out of 2 Total Num of Address Entries displayed
```

Displaying IPv6 interface addresses

View IPv6 interface addresses to learn the addresses.

Prerequisites

Log on to the User EXEC mode in ACLI.

Display IPv6 interface addresses

Use the following command to display IPv6 interface addresses:

`show ipv6 address interface [vlan <1-4094> | <WORD 0-45>]`

Variable definitions

The following table list the variables and definitions.

Variable	Definition
address-type <1-2>	Address type
name <1-255>	Name: integer from 1–255
link-local <WORD 0-19>	Local link
mtu <1280-9600>	Default status: MTU 1280
reachable-time <0-3600000>	Time in milliseconds neighbor is considered reachable after a reachable confirmation message. Default: 30000
retransmit-timer <0-3600000>	Time in milliseconds between retransmissions of neighbor solicitation messages to a neighbor. Default: 1000
enable	Enables the interface administrative status.

Configuring an IPv6 address for a switch or stack

Use the following procedure to configure an IPv6 address for a switch or stack:

ipv6 address

Enter the following command:

```
ipv6 address {[<ipv6_address/prefix_length>] [stack
<ipv6_address/prefix_length>] [switch <ipv6_address/
prefix_length>] [unit <1-8> <ipv6_address/prefix_length>]}
```

Variable definitions

The following table defines the variables used to configure an IPv6 address for a switch or stack.

Variable	Definition
`ipv6_address/prefix_length`	
`stack`	IP address of stack
`switch`	IP address of switch
`unit`	Unit number: 1-8

Displaying the IPv6 address for a switch or stack

Use the following procedure to display the IPv6 address for a switch or stack:

show ipv6 address

Enter the following command:

```
show ipv6 address
```

show ipv6 address interface

Enter the following command to display all or a specific ipv6 interface address.

```
show ipv6 address interface <ipv6_address>
```

Job aid

The following graphic shows the results of the**`show ipv6 address interface`** command.

```
4526(config)#show ipv6 address interface
=====================================================================================
                                        Address Information
=====================================================================================
IPV6 ADDRESS                            VID/BID/  TYPE      ORIGIN    STATUS
                                        TID
-------------------------------------------------------------------------------------
3000:0:0:0:0:0:0:99                     V-1       UNICAST   MANUAL    PREFERRED
fe80:0:0:0:211:f9ff:fe34:8800           V-1       UNICAST   OTHER     UNKNOWN
2out of 2Total Num of Address Entries displayed.
```

Configuring IPv6 interface properties

Use the following procedure to configure the IPv6 interface, create the VLAN IPv6 interface, and set the parameters

Enter the following command:

```
ipv6 interface [address <ipv6_address/prefix_length>]
```

Variable definitions

Use the data in the following table to help you use the **show ipv6 address interface** command.

Variable	Definition
vlan <1-4094>	Specifies a specific VLAN for which to display IPv6 addresses.
<WORD 0-45>	Specifies the IPv6 address and prefix to be displayed.

The following table shows the field descriptions for this command.

Table 43: show ipv6 address interface command field descriptions

Field	Description
IPV6 ADDRESS	Specifies the IPv6 destination address.
TYPE	Specifies Unicast, the only supported type.
ORIGIN	Specifies a read-only value indicating the origin of the address. The origin of the address is other, manual, DHCP, linklayer, or random.
STATUS	Indicates the status of the IPv6 address. The values of the status are as follows: • PREFERRED • DEPRECATED • INVALID • INACCESSIBLE • UNKNOWN • TENTATIVE • DUPLICATE
VID/BID/TID	Specifies the VLAN ID corresponding with the IPv6 address configured.

Disabling IPv6 interface

Use the following procedure to disable the IPv6 interface:

Enter the following command to disable IPv6.

```
no ipv6 interface [address <ipv6_address>] [all] [enable]
```

Displaying the global IPv6 configuration

Use the following procedure to display the IPv6 global configuration:

Enter the following command to display the global IPv6 configuration.

```
show ipv6 global
```

Job aid

The following graphic shows a possible result of the **show ipv6 global** command.

```
4526(config)#show ipv6 global
forwarding              : disabled
default-hop-cnt         : 30
number-of-interfaces    : 1
admin-status            : enabled
icmp-error-interal      : 1000
icmp-error quota        : 50
icmp-redirect-msg       : disabled
icmp-unreach-msg        : disabled
multicast-admin-status  : disabled
```

The following table describes the default settings for the fields in the graphic.

Field	Default setting
forwarding	disabled
default-hop-cnt	30
number-of-interfaces	1
admin-status	enabled

Field	Default setting
icmp-error-interval	1000
icmp-error-quota	50
icmp-redirect-msg	disabled
icmp-unreach-msg	disabled
multicast-admin-status	disabled

Configuring an IPv6 default gateway for the switch or stack

1. Enter the following command to configure a default gateway.

   ```
   ipv6 default-gateway <ipv6_gateway address>
   ```

2. Enter the following command to disable a default gateway.

   ```
   no ipv6 default-gateway
   ```

Displaying the IPv6 default gateway

Use the following procedure to display the IPv6 address for the default gateway:

Enter the following command:

```
show ipv6 default-gateway
```

Configuring the IPv6 neighbor cache

Use the following procedure to add or remove a static neighbor cache entry:

1. Enter the following command to add a static neighbor cache entry.

   ```
   ipv6 neighbor <ipv6_address> port <unit/port> mac <H.H.H>
   ```

2. Enter the following command to remove a static neighbor cache entry.

   ```
   no ipv6 neighbor <ipv6_address>
   ```

Displaying the IPv6 neighbor information

Use the following command to display IPv6 neighbor information:

Enter the following command to display the address and status of the neighbor cache.

```
show ipv6 neighbor [<ipv6_address>] [type {other | dynamic | static | local}]
```

Job aid

The following graphic shows the output of the **show ipv6 neighbor** command.

```
4526(config)#show ipv6 neighbor
==========================================================================================
                                  Neighbor Information
==========================================================================================
NET ADDRESS/ PHYSICAL ADDRESS              PHYS INTF  TYPE    STATE      LAST
                                                                         UPD
------------------------------------------------------------------------------------------
3000:0:0:0:0:0:0:0/ 00:11:F9:34:88:00      V-1        LOCAL   REACHABLE  0
3000:0:0:0:0:0:0:1/ 00:01:02:03:04:05      1/5        STATIC  REACHABLE  387452
3000:0:0:0:0:0:0:99/ 00:11:f9:34:88:00     V-1        LOCAL   REACHABLE  385251
fe80:0:0:0:211:f9ff:fe34:8800/ 00:11:f9:34:88:00  V-1  LOCAL  REACHABLE  385193
```

Displaying IPv6 interface ICMP statistics

Use the following procedure to display IPv6 interface ICMP statistics:

Enter the following command:

```
show ipv6 interface icmpstatistics [<1-4094>]
```

Job aid

The following graphic shows a sample of the results from the **show ipv6 interface icmpstatistics** command.

```
4526(config)#show ipv6 interface icmpstatistics
================================================================================
                                   Icmp Stats
================================================================================
Icmp stats for IfIndex = 10001
IcmpInMsgs: 1
IcmpInErrors: 1
IcmpInDestUnreachs: 1
IcmpInAdminProhibs: 0
IcmpInTimeExcds: 0
IcmpInParmProblems: 0
IcmpInPktTooBigs: 0
IcmpbInEchos: 0
IcmpInEchoReplies: 0
<truncated>
```

Displaying IPv6 interface statistics

Enter the following command:

`show ipv6 interface statistics`

Job aid

The following graphic shows a sample of the results from the **`show ipv6 interface statistics`** command.

```
4526(config)# show ipv6 interface statistics
================================================================================
                                      Interface Stats
================================================================================
IF stats for IfIndex = 10001
InReceives: 0
InHdrErrors: 0
```

InTooBigErrors: 0
InNoRoutes: 0
InAddrErrors: 0
InUnknownProtos: 0
InTruncatedPkts: 0
InDiscards: 0
InDelivers: 20
<truncated>

Displaying IPv6 TCP statistics

Use the following procedure to display IPv6 TCP statistics:

show ipv6 tcp

Enter **`show ipv6 tcp`** to display the TCP statistics for IPv6.

Job aid

The following graphic shows a sample result from the **`show ipv6 tcp`** command.

4526(config)# show ipv6 tcp	
show ipv6 tcp global statistics:	
--	
ActiveOpens:	0
PassiveOpens:	0
AttemptFails:	0
EstabResets:	0
CurrEstab:	1
InSegs:	24
OutSegs:	20
RetransSegs:	2
InErrs:	0
OutRsts:	0
HCInSegs:	24

HCOutSegs:	20

Displaying IPv6 TCP connections

Use the following procedure to display IPv6 TCP connections:

Enter the following command:

```
show ipv6 tcp connections
```

Displaying IPv6 TCP listeners

Use the following procedure to display IPv6 TCP listeners:

Enter the following command:

```
show ipv6 tcp listener
```

Displaying IPv6 UDP statistics and endpoints

Use the following procedure to display IPv6 UDP statistics and endpoints:

1. Enter the following command to show UDP statistics.

   ```
   show ipv6 udp
   ```

2. Enter the following command to show UDP endpoints.

   ```
   show ipv6 udp endpoints
   ```

Configuring PoE using ACLI

The following section describes the commands necessary to configure PoE using ACLI:

- Set port power enable or disable on page 126
- Set port power priority on page 126
- Set power limit for channels on page 127
- Set traps control on page 127
- Show main power status on page 127
- Set power usage threshold on page 128

- Setting PoE detection method on page 128
- Show port power status on page 128
- Show port power measurement on page 129

Set port power enable or disable

Use the **poe-shutdown command** to disable PoE to a port.

The syntax for the poe-shutdown command is

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

Use the **no poe-shutdown** command to enable PoE to a port.

The syntax for the **no poe-shutdown** command is

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

In either command, substitute **<portlist>** with the ports on which PoE is enabled or disabled.

Run the **poe-shutdown** and **no poe-shutdown** commands in Interface Configuration command mode.

Set port power priority

The **poe-priority** command sets the port power priority.

The syntax for the **poe-priority** command is

```
poe poe-priority [port <portlist>] {critical | high | low}
```

Table 44: poe-priority parameters on page 126 outlines the parameters for this command.

Table 44: poe-priority parameters

Parameter	Description
port <portlist>	The ports to set priority for
{low | high | critical}	The PoE priority for the port

Run the **poe-priority** command in Interface Configuration command mode.

Set power limit for channels

The **poe-limit** command sets the power limit for channels.

The syntax for the **poe-limit** command is

`poe poe-limit [port <portlist>] <3-16>`

Table 45: poe-limit parameters on page 127 outlines the parameters for this command.

Table 45: poe-limit parameters

Parameter	Description
port <portlist>	The ports to set the limit on
<3 - 16>	The power range to limit at from 3 to 16 W

Run the **poe-limit** command in Interface Configuration command mode.

Set traps control

The **poe-trap** command enables PoE-related traps for PoE-enabled ports.

The syntax for the **poe-trap** command is

`poe poe-trap [unit <1-8>]`

Substitute **<1-8>** with the number of the unit on which to enable traps.

Show main power status

The **show poe-main-configuration** command displays the power configuration.

The syntax for the **show poe-main-configuration** command is

`show poe-main-status [unit <1-8>]`

Substitute `<1-8>` with the number of the unit for which to display the configuration.

Run the **show poe-main-status** command in Privileged EXEC command mode.

Set power usage threshold

The **poe-power-usage-threshold** command sets the power usage threshold in percentage on individual units.

By setting the PoE power threshold, you can set a percentage of the total PoE power usage at which the switch sends a warning trap message. If the PoE power usage exceeds the threshold and SNMP traps are configured appropriately, the switch sends the pethMainPowerUsageOnNotification trap. If the power consumption exceeds and then falls below the threshold, the switch sends the pethMainPowerUsageOffNotification trap.

The syntax for the **poe-power-usage-threshold** command is

```
poe poe-power-usage-threshold [unit <1-8>] <1-99>
```

Table 46: poe-power-usage-threshold parameters on page 128 outlines the parameters for this command.

Table 46: poe-power-usage-threshold parameters

Parameter	Description
unit <1 - 8>	The unit for which to set the power threshold.
<1 - 99>	1—99 percent

Run the **show poe-main-configure** command in Global Configuration command mode.

Setting PoE detection method

The **poe-pd-detect-type** command enables either 802.3af or Legacy compliant PD detection methods.

The syntax for the **poe-pd-detect-type 802dot3af_and_legacy** command is

```
poe poe-pd-detect-type [unit <1-8>] {802dot3af |
802dot3af_and_legacy}
```

Run the **poe-pd-detect-type 802dot3af_and_legacy** command in Global Configuration command mode.

Show port power status

The **show port power status** command displays the power configuration.

The syntax for the **show port power status** command is

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

Substitute **<portlist>** with the ports for which to display configuration.

Run the **show poe-port-status** command in Global Configuration command mode.

Show port power measurement

The **show port power measurement** command displays the power configuration.

The syntax for the **show port power measurement** command is:

```
show poe-power-measurement [<portlist>]
```

Substitute <portlist> with the ports for which to display configuration.

Run the **show poe-power-measurement** command in Global Configuration command mode.

General switch administration using ACLI

This section describes the ACLI commands used in general switch administration. This section contains the following topics:

- Connecting to Another Switch on page 159
- Domain Name Server (DNS) Configuration on page 160
- Serial Security on page 163

Multiple switch configurations

The Avaya Ethernet Routing Switch 4500 Series supports the storage of two switch configurations in flash memory. The switch can use either configuration and must be reset for the configuration change to take effect.

A regular reset of the switch synchronizes configuration changes to the active configuration, whereas a reset to defaults sets configuration 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 active configuration and the stack active configuration. If the two differ, the new stack unit resets and loads the stack active configuration.

The following considerations apply to NVRAM commands:

- The Nvram block that is not active is not reset to default after downgrade.
- You can save the switch binary configuration to the non-default NVRAM block.
- When you perform an agent code downgrade on the switch, only the configuration from the default block resets to default.

Use the following ACLI commands to configure and use multiple switch configuration:

- show nvram block command on page 130
- copy config nvram block command on page 131
- copy nvram config block command on page 131

show nvram block command

This command shows the configurations currently stored on the switch. The syntax for this command is

```
show nvram block
```

Example

```
show nvram block

 Block Active Name Last Saved
-------------------------------------------------
1 True   Configuration_Block_1
2 False  α
```

Important:

The Last Saved time is not available even if SNTP is active. ERS4500 switch does not have a RTC (Real Time Clock).

Run this command in Global Configuration command mode.

copy config nvram block command

This command copies the current configuration to one of the flash memory locations. The syntax for this command is

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

Table 47: copy config nvram block parameters on page 131 outlines the parameters for this command.

Table 47: copy config nvram block parameters

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

Run this command in Global Configuration command mode.

copy nvram config block command

This command copies the configuration stored in flash memory at the specified location and makes it the active configuration. The syntax for this command is

```
copy nvram config block <1-2>
```

Substitute `<1-2>` with the configuration file to load.

This command resets the switch to reset so that the new configuration load.

Run this command in Global Configuration command mode.

Configuring system IP addresses and boot mode

Configure, clear, and view IP addresses, gateway addresses, and boot mode information . For details, see:

- ip address command on page 132
- default ip address command on page 133

ip address command

The **ip address** command sets the IP address and subnet mask for the switch or a stack, and selects BootP or DHCP as the boot mode for the next switch reboot.

The syntax for the **ip address** command is

```
ip address <A.B.C.D> [netmask <A.B.C.D>] source {bootp-always|bootp-last-address|bootp-when-needed|configured-address|dhcp-always|dhcp-last-address|dhcp-when-needed} [stack|switch|unit]
```

Run the **ip address** command in Global Configuration command mode.

If the stack or switch parameter is not specified, the system automatically modifies the stack IP address when in stack mode and modifies the switch IP address when in standalone mode.

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

Table 48: ip address parameters

Parameters	Description
A.B.C.D	Specifies the IP address in dotted-decimal notation.
netmask	Specifies the IP subnet mask for the stack or switch. The netmask is optional.
source	Specifies whether to use the BootP or DHCP server to assign an IPv4 address for the management VLAN at the next switch reboot. Values include: • bootp-always—always use the BootP server • bootp-last-address—use the BootP server last used • bootp-when-needed—use the BootP server when needed

Parameters	Description
	• configured-address—use configured server IP address • dhcp-always—always use the DHCP server • dhcp-last-address—use the DHCP server last used • dhcp-when-needed—use the DHCP server when needed
stack | switch | unit	Specifies the IP address and netmask of the stack or the switch, or another unit in at a stack.

Important:
When you change the IP address or subnet mask, connectivity to Telnet and the Web can be lost.

default ip address command

The **`default ip address`** command sets the IP address, subnet mask, and boot mode for the switch or a stack to default.

The syntax for the **`default ip address [source]`** command is

```
default ip address
```

Run the **`default ip address`** command in Global Configuration command mode.

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

Table 49: default ip address parameters

Variable	Value
source	Configures the BootP and DHCP boot mode to default for the next system reboot.

Important:
When the IP gateway changes, connectivity to Telnet and the Internet can be lost.

no ip address command

The **`no ip address`** command clears the IP address and subnet mask for a switch or a stack. This command sets the IP address and subnet mask for a switch or a stack to all zeros (0).

The syntax for the **`no ip address`** command is

```
no ip address {stack | switch | unit}
```

Run the **no ip address** command in Global Configuration command mode.

The following table describes the parameters for this command.

Table 50: no ip address parameters

Parameters	Description
stack | switch	Zeroes out the stack IP address and subnet mask or the switch IP address and subnet mask.
unit	Zeroes out the IP address for the specified unit.

Important:

When you change the IP address or subnet mask, connectivity to Telnet and the Web Interface can be lost. Any new Telnet connection can be disabled and must connect to the serial console port to configure a new IP address.

show ip address source command

The **show ip address source** command displays the configured boot mode for the next switch reboot.

The syntax for the **show ip address source** command is

```
show ip address source
```

Run the **show ip address source** command in User EXEC or Privileged EXEC command mode.

ip dhcp client lease command

The **ip dhcp client lease** command configures the DHCP client lease time in seconds, minutes, hours, days, and weeks.

The syntax for the **ip dhcp client lease <time>** command is

```
ip dhcp client lease
```

Run the **ip dhcp client lease** command in Global Configuration command mode.

The following table describes the parameters for the **ip dhcp client lease** command.

Table 51: ip dhcp client lease parameters

Variable	Value
<time>	Specifies the DHCP client lease time. Values include:

Variable	Value
	• seconds—from 10–4294967295 • minutes—from 1–71582788 • hours—from 1–1193046 • days—from 1–49710 • weeks—from 1–7101

Important:

When you change the IP address or subnet mask, connectivity to Telnet and the Web can be lost.

default ip dhcp client lease command

The **`default ip dhcp client lease`** command configures the DHCP client lease time (seconds, minutes, hours, days, and weeks) to default values.

The syntax for the **`default ip dhcp client lease`** command is

```
default ip dhcp client lease
```

Run the **`default ip dhcp client lease`** command in Global Configuration command mode.

Important:

When you change the IP address or subnet mask, connectivity to Telnet and the Web can be lost.

no ip dhcp client lease command

The **`no ip dhcp client lease`** command deletes the DHCP client lease time.

The syntax for the **`no ip dhcp client lease`** command is

```
no ip dhcp client lease
```

Run the **`no ip dhcp client lease`** command in Global Configuration command mode.

show ip dhcp client lease command

The **`show ip dhcp client lease`** command displays the configured and granted DHCP client lease time.

The syntax for the **show ip dhcp client lease** command is

```
show ip dhcp client lease
```

Run the **no ip dhcp client lease** command in User EXEC or Privileged EXEC command mode.

renew dhcp command

The **renew dhcp** command renews the DHCP client lease.

The syntax for the **renew dhcp** command is

```
renew dhcp
```

Run the **renew dhcp** command in Global Configuration command mode.

ip default-gateway command

The **ip default-gateway** command sets the default IP gateway address for a switch or a stack to use.

The syntax for the **ip default-gateway** command is

```
ip default-gateway <XXX.XXX.XXX.XXX>
```

Run the **ip default-gateway** command in Global Configuration command mode.

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

Table 52: ip default-gateway parameters

Parameters	Description
XXX.XXX.XXX.XXX	Enter the dotted-decimal IP address of the default IP gateway.

Important:
When you change the IP gateway, connectivity to Telnet and the Web Interface can be lost.

no ip default-gateway command

The **no ip default-gateway** command sets the IP default gateway address to zero (0).

The syntax for the **no ip default-gateway** command is

```
no ip default-gateway
```

Run the **no ip default-gateway** command in Global Configuration command mode.

Important:
When you change the IP gateway, connectivity to Telnet and the Web Interface can be lost.

show ip command

The **show ip** command displays the IP configurations, BootP mode, stack address, switch address, subnet mask, and gateway address. This command displays these parameters for what is configured, what is in use, and the last BootP. The sub command, **Display DNS configuration**, provides information about the DNS configuration.

The syntax for the **show ip** command is

```
show ip [bootp] [default-gateway] [address]
```

Run the **show ip** command in User EXEC or Privileged EXEC command mode.

If you do not enter any parameters, this command displays all IP-related configuration information.

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

Table 53: show ip parameters

Variables	Description
bootp	BootP-related IP information.
default-gateway	The IP address of the default gateway.
address	The current IP address.

Assigning and clearing IP addresses for specific units

You can use ACLI to assign and clear IP addresses for a specific unit in a stack. For details, see the following sections:

- ip address unit command on page 137
- no ip address unit command on page 138

ip address unit command

The **ip address unit** command sets the IP address and subnet mask of a specific unit in the stack.

The syntax for the **`ip address unit`** command is

```
ip address unit <1-8> [A.B.C.D]
```

Run the **`ip address unit`** command in Global Configuration command mode.

The following table describes the parameters this command.

Table 54: ip address unit parameters

Parameters and variables	Description
unit <1—8>	Sets the unit you are assigning an IP address.
A.B.C.D	Enter IP address in dotted-decimal notation.

Important:
When the IP address or subnet mask changes, connectivity to Telnet and the Internet can be lost.

no ip address unit command

The **`no ip address unit`** command sets the IP address for the specified unit in a stack to zeros (0).

The syntax for the **`no ip address unit`** command is

```
no ip address unit <1-8>
```

Run the **`no ip address unit`** command in Global Configuration command mode.

The following table describes the parameters this command.

Table 55: no ip address parameters

Variable	Value
unit <1—8>	Zeroes out the IP address for the specified unit.

Important:
When you change the IP address or subnet mask, connectivity to Telnet and the Internet can be lost.

Displaying Interfaces

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

show interfaces command

The **show interfaces** command displays the current configuration and status of all interfaces.

The syntax for the **show interfaces** command is

`show interfaces [names] [<portlist>] [gbic-info]`

Run the **show interfaces** command in User EXEC command mode.

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

Table 56: show interfaces variables

Variables	Description
names <portlist>	Display interface names; enter specific ports to see only those ports.
gbic-info	Display GBIC details.
LINE	Display a list of existing ports with names (displays interface names).

Displaying configuration information for ports

The show port enhancement provides the ability to show all the configuration information for a specific port through ACLI.

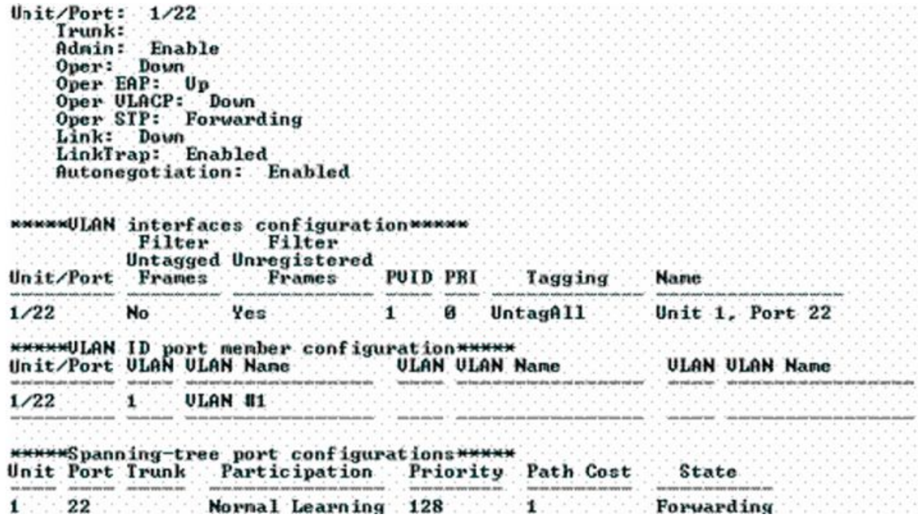
The syntax for the show port enhancement command is: .

`show interfaces <portlist> config`

The command displays information related to port configuration, VLAN interface, VLAN port member, and Spanning-Tree configuration.

The following example displays sample output for the show port enhancement:

`show interfaces 1/22 config`



```
Unit/Port:  1/22
    Trunk:
    Admin:  Enable
    Oper:  Down
    Oper EAP:  Up
    Oper VLACP:  Down
    Oper STP:  Forwarding
    Link:  Down
    LinkTrap:  Enabled
    Autonegotiation:  Enabled

*****VLAN interfaces configuration*****
           Filter      Filter
          Untagged Unregistered
Unit/Port  Frames      Frames    PVID PRI    Tagging     Name
1/22      No       Yes           1    0   UntagAll      Unit 1, Port 22

*****VLAN ID port member configuration*****
Unit/Port VLAN VLAN Name           VLAN VLAN Name           VLAN VLAN Name
1/22      1    VLAN #1

*****Spanning-tree port configurations*****
Unit Port Trunk  Participation   Priority  Path Cost    State
1    22          Normal Learning 128       1            Forwarding
```

Setting port speed

To set port speed and duplexing using ACLI, see the following sections:

- speed command on page 140
- default speed command on page 141
- duplex command on page 141
- default duplex command on page 142

speed command

The **speed** command sets the port speed.

The syntax for the **speed** command is

```
speed [port <portlist>] {10 | 100 | 1000 | auto}
```

Run the **speed** command in Interface Configuration command mode.

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

Table 57: speed variables

Variables	Description
port <portlist>	Specify the port numbers to configure the speed. Enter the port numbers you want to configure.

Variables	Description
	Important: If you omit this parameter, the system uses the port number you specified in the **interface** command.
10|100|1000|auto	Set the speed to: • 10: 10 Mb/s • 100: 100 Mb/s • 1000: 1000 Mb/s or 1 GB/s • auto: autonegotiation

Important:

Enabling or disabling autonegotiation for speed also enables or disables it for duplex operation.

When you set the port speed for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

default speed command

The **default speed** command sets the port speed to the factory default speed.

The syntax for the **default speed** command is

```
default speed [port <portlist>]
```

Run the **default speed** command in Interface Configuration command mode.

The following table describes the parameters for this command.

Table 58: Default speed variables

Variables	Description
port <portlist>	Specify the port numbers for which to set the speed to factory default. Enter the port numbers to set. **Important:** If you omit this parameter, the system uses the port number you specified in the **interface** command.

duplex command

The **duplex** command specifies the duplex operation for a port.

The syntax for the **duplex** command is

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

Run the **duplex** command in Interface Configuration command mode.

The following table describes the parameters for this command.

Table 59: Duplex variables

Variables	Description
port <portlist>	Specify the port numbers to reset the duplex mode to factory default values. Enter the port number to configure. The default value is autonegotiation. **Important:** If you omit this parameter, the system uses the ports you specified in the **interface** command.
full | half | auto	Set duplex to • full: full-duplex mode • half: half-duplex mode • auto: autonegotiation

Important:

Enabling or disabling autonegotiation for speed also enables or 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 command

The **default duplex** command sets the duplex operation for a port to the factory default duplex value.

The syntax for the **default duplex** command is

```
default duplex [port <portlist>]
```

Run the **default duplex** command in Interface Configuration command mode.

The following table describes the parameters for this command.

Table 60: Default duplex variables

Variables	Description
port <portlist>	Specify the port numbers for which to reset the duplex mode to factory default values. Enter the port numbers to configure. The default value is autonegotiation. **Important:** If you omit this parameter, the system uses the ports you specified in the **interface** command.

Initiating a cable diagnostic test using ACLI

Use the information in this section to initiate and display results for a cable diagnostic test globally, or for one or more specific switch ports, using the Time Domain Reflectometer (TDR).

tdr test command

The **tdr test** command initiates a cable diagnostic test globally, or for one or more specific switch ports.

The syntax for the **tdr test** command is

```
tdr test <portlist>
```

Run the **tdr test** command in Privileged EXEC command mode.

Variable definitions

The following table defines optional parameters that you can enter after the **tdr test** command.

Variable	Value
<WORD>	Specifies a port or list of ports.

show tdr test command

The **show tdr test** command displays cable diagnostic test results globally, or for one or more specific switch ports.

The syntax for the **show tdr test** command is

```
show tdr test <portlist>
```

Run the **show tdr test** command in Privileged EXEC command mode.

Variable definitions

The following table defines optional parameters that you can enter after the **show tdr test** command.

Variable	Value
<WORD>	Specifies a port or list of ports.

Enabling Autotopology

Use ACLI to configure the Enterprise Autotopology protocol.

For more information about Autotopology, see http://www.avaya.com. (The product family for Enterprise and Autotopology is Data and Internet.)

To enable autotopology using ACLI, see the following sections:

- autotopology command on page 144
- no autotopology command on page 144
- default autotopology command on page 145
- show autotopology settings command on page 145
- show autotopology nmm-table command on page 145

autotopology command

The **autotopology** command enables the Autotopology protocol.

The syntax for the **autotopology** command is

```
autotopology
```

Run the **autotopology** command in Global Configuration command mode.

no autotopology command

The **no autotopology** command disables the Autotopology protocol.

The syntax for the **no autotopology** command is

```
no autotopology
```

Run the **no autotopology** command in Global Configuration command mode.

default autotopology command

The **default autotopology** command enables the Autotopology protocol.

The syntax for the **default autotopology** command is

```
default autotopology
```

Run the **default autotopology** command in Global Configuration command mode.

The **default autotopology** command has no parameters or values.

show autotopology settings command

The **show autotopology settings** command displays the global autotopology settings.

The syntax for the **show autotopology settings** command is

```
show autotopology settings
```

Run the **show autotopology settings** command in Privileged EXEC command mode.

The **show autotopology settings** command has no parameters or values.

show autotopology nmm-table command

The **show autotopology nmm-table** displays the Autotopology network management module (NMM) table.

The syntax for the **show autotopology nmm-table** command is

```
show autotopology nmm-table
```

Run the **show autotopology nmm-table** command in Privileged EXEC command mode.

The **show autotopology nmm-table** command has no parameters or values.

Enabling flow control

Gigabit Ethernet, when used with the Avaya Ethernet Routing Switch 4500 Series, can control traffic on this port using the **flowcontrol** command.

Important:
Due to Quality of Service (QoS) interaction, the switch; cannot send pause-frames.

To enable flow control using ACLI, see the following sections:

- flowcontrol command on page 146
- no flowcontrol command on page 146
- default flowcontrol command on page 147

flowcontrol command

Use the **flowcontrol** command only on Gigabit Ethernet ports to control the traffic rates during congestion.

The syntax for the **flowcontrol** command is

```
flowcontrol [port <portlist>] {asymmetric | symmetric | auto |
disable}
```

Run the **flowcontrol** command in Interface Configuration mode.

The following table describes the parameters for this command.

Table 61: Flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers to configure for flow control. **Important:** If you omit this parameter, the system uses the ports you specified in the **interface** command but only those ports that have speed set to 1000/full.
asymmetric | symmetric | auto | disable	Set the mode for flow control: • asymmetric: PAUSE frames can flow only in one direction. • symmetric: PAUSE frames can flow in either direction. • auto: Set the port to automatically determine the flow control mode (default). • disable: Disable flow control on the port.

no flowcontrol command

Use the **no flowcontrol** command only on Gigabit Ethernet ports to disable flow control.

The syntax for the **no flowcontrol** command is

```
no flowcontrol [port <portlist>]
```

Run the **no flowcontrol** command in Interface Configuration mode.

The following table describes the parameters for this command.

Table 62: No flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers for which to disable flow control. **Important:** If you omit this parameter, the system uses the ports you specified in the **interface** command, but only those ports that have speed set to 1000/full.

default flowcontrol command

Use the **default flowcontrol** command only on Gigabit Ethernet ports to set the flow control to automatic, which automatically detects the flow control.

The syntax for the **default flowcontrol** command is

```
default flowcontrol [port <portlist>]
```

Run the **default flowcontrol** command in Interface Configuration mode.

The following table describes the parameters for the command.

Table 63: Default flowcontrol parameters

Parameters and variables	Description
port <portlist>	Specify the port numbers to default to automatic flow control. **Important:** If you omit this parameter, the system uses the port number you specified in the **interface** command.

Enabling rate-limiting

The percentage of multicast traffic, or broadcast traffic, or both, can be limited using ACLI. For details, see the following sections:

- show rate-limit command on page 148
- rate-limit command on page 148

- no rate-limit command on page 149
- default rate-limit command on page 149

show rate-limit command

The **show rate-limit** command displays the rate-limiting settings and statistics.

The syntax for the **show rate-limit** command is

```
show rate-limit
```

Run the **show rate-limit** command in Privileged EXEC command mode.

rate-limit command

The **rate-limit** command configures rate-limiting on the port.

The syntax for the **rate-limit** command is

```
rate-limit [port <portlist>] {multicast <pct> | broadcast <pct> |
both <pct>}
```

Run the **rate-limit** command in Interface Configuration command mode.

The following table describes the parameters for this command.

Table 64: Rate-limit parameters

Parameters and values	Description
port <portlist>	Specify the port numbers to configure for rate-limiting. Enter the port numbers to configure. **Important:** If you omit this parameter, the system uses the port number you specified in the **interface** command.
multicast <pct> | broadcast <pct> | both <pct>	Apply rate-limiting to the type of traffic. Enter an integer from 1–10 to set the rate-limiting percentage: • multicast: Apply rate-limiting to multicast packets. • broadcast: Apply rate-limiting to broadcast packets. • both: Apply rate-limiting to both multicast and broadcast packets.

no rate-limit command

The **no rate-limit** command disables rate-limiting on the port.

The syntax for the **no rate-limit** command is:

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

Run the **no rate-limit** command in Interface Configuration command mode.

The following table describes the parameters for this command.

Table 65: No rate-limit parameters

Parameters	Description
port <portlist>	Specify the port numbers to disable for rate-limiting. Enter the port numbers to disable. **Important:** If you omit this parameter, the system uses the port number you specified in the **interface** command.

default rate-limit command

The **default rate-limit** command restores the rate-limiting value for the specified port to the default setting.

The syntax for the **default rate-limit** command is

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

Run the **default rate-limit** command in Interface Configuration command mode.

The following table describes the parameters for this command.

Table 66: Default rate-limit parameters

Parameters	Description
port <portlist>	Specify the port numbers to reset rate-limiting to factory default. Enter the port numbers to set rate-limiting to default. **Important:** If you omit this parameter, the system uses the port number you specified in the **interface** command.

Using Simple Network Time Protocol

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

Important:

If problems occur when you use this feature, 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.

Use SNTP to provide a real-time timestamp for the software, shown as Greenwich Mean Time (GMT).

If you run SNTP, 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 does not occur 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.

To configure SNTP, see the following commands:

- Show SNTP command on page 150
- show sys-info command on page 151
- SNTP enable command on page 151
- No SNTP enable command on page 151
- SNTP server primary address command on page 151
- SNTP server secondary address command on page 152
- No SNTP server command on page 152
- SNTP sync-now command on page 153
- SNTP sync-interval command on page 153

Show SNTP command

The **show SNTP** command displays the SNTP information, as well as the configured NTP servers.

The syntax for the **show SNTP** command is

```
show sntp
```

Run the **show SNTP** command in Privileged EXEC command mode.

show sys-info command

The **show sys-info** command displays the current system characteristics.

The syntax for the **show sys-info** command is

```
show sys-info
```

Run the **show sys-info** command in Privileged EXEC command mode.

Important:
You must have SNTP enabled and configured to display GMT time.

SNTP enable command

The **SNTP enable** command enables SNTP.

The syntax for the **SNTP enable** command is

```
sntp enable
```

Run the **SNTP enable** command in Global Configuration command mode.

Important:
The default setting for SNTP is Disabled.

No SNTP enable command

The **no SNTP enable** command disables SNTP.

The syntax for the **no SNTP enable** command is

```
no sntp enable
```

Run the **no SNTP enable** command in Global Configuration command mode.

SNTP server primary address command

The **SNTP server primary address** command specifies the IP addresses of the primary NTP server.

The syntax for the **SNTP server primary address** command is

```
sntp server primary address [<ipv6_address> | <A.B.C.D>]
```

Run the **SNTP server primary address** command in Global Configuration command mode.

The following table describes the parameters for this command.

Table 67: SNTP server primary address parameters

Parameters and Variables	Description
ipv6_address	Enter the IPv6 address of the primary NTP server.
<A.B.C.D>	Enter the IP address of the primary NTP server in dotted-decimal notation.

SNTP server secondary address command

The **SNTP server secondary address** command specifies the IP addresses of the secondary NTP server.

The syntax for the **SNTP server secondary address** command is

```
sntp server secondary address [<ipv6_address> | <A.B.C.D>]
```

Run the **SNTP server secondary address** command in Global Configuration command mode.

The following table describes the parameters for this command.

Table 68: SNTP server secondary address parameters

Parameters	Description
ipv6_address	Enter the IPv6 address of the secondary NTP server.
<A.B.C.D>	Enter the IP address of the secondary NTP server in dotted-decimal notation.

No SNTP server command

The **no SNTP server** command clears the NTP server IP addresses. The command clears the primary and secondary server addresses.

The syntax for the **no SNTP server** command is

```
no sntp server {primary | secondary}
```

Run the **no SNTP server** command in Global Configuration command mode.

The following table describes the parameters for this command.

Table 69: no SNTP server parameters

Parameters	Description
primary	Clear the primary SNTP server address.
secondary	Clear the secondary SNTP server address.

SNTP sync-now command

The **`SNTP sync-now`** command forces a manual synchronization with the NTP server.

The syntax for the **`SNTP sync-now`** command is

```
sntp sync-now
```

Run the **`SNTP sync-now`** command in Global Configuration command mode.

Important:
SNTP must be enabled before this command can take effect.

SNTP sync-interval command

The **`SNTP sync-interval`** command specifies recurring synchronization with the secondary NTP server in hours relative to initial synchronization.

The syntax for the **`SNTP sync-interval`** command is

```
sntp sync-interval <0-168>
```

Run the **`SNTP sync-interval`** command in Global Configuration command mode.

The following table describes the for this command.

Table 70: SNTP sync-interval parameters

Parameters and Variables	Description
<0-168>	Enter the number of hours for periodic synchronization with the NTP server. **Important:** 0 is boot-time only, and 168 is once a week.

Configuring local time zone

Use the following procedure to configure your switch for your local time zone.

1. In ACLI, set the global configuration mode.

   `configure`

2. Enable sntp server.
3. Set clock time zone using the clock command.

   `clock time-zone zone hours [minutes]`

Parameters	Description
zone	Time zone acronym to be displayed when showing system time (up to 4 characters).
hours	Difference from UTC in hours. This can be any value between -12 and +12.
minutes	Optional: This is the number of minutes difference from UTC. Minutes can be any value between 0 and 59.

Setting time zone example

`clock time-zone PST -8`

This command sets the time zone to UTP minus 8 hours and the time zone will be displayed as "PST."

Configuring daylight savings time

Use the following procedure to configure local daylight savings time recurring change dates.

1. In ACLI, set the global configuration mode.

   `configure terminal`

2. Enable sntp server.
3. Set the date to change to daylight savings time.

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

Variables	Description
date	Indicates that daylight savings time you set to start and end on the specified days every year.
day	Date to start daylight savings time.
month	Month to start daylight savings time.
year	Year to start daylight savings time.
hh:mm	Hour and minute to start daylight savings time.
day	Date to end daylight savings time.
month	Month to end daylight savings time.
year	Year to end daylight savings time.
hh:mm	Hour and minute to end daylight savings time.
offset	Number of minutes to add during the summer time.
zone	The time zone acronym to be displayed when daylight savings time is in effect. If it is unspecified, it defaults to the time zone acronym set when the time zone was set.

set daylight savings time example

```
clock summer-time BST date 28 Mar 2007 2:00 30 Aug 2007 15:00 +60
```

This command sets the daylight savings time to begin at 02:00 on March 28, 2007 and end on August 30th, 2007 at 15:00. The change to daylight savings moves the clock forward by 60 minutes and "BST" will be displayed as the time zone acronym. These changes to and from daylight savings time will happen automatically.

Configuring recurring daylight savings time

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

1. In ACLI, set the global configuration mode.
2. Enable the SNTP server.
3. Set the date to change to daylight savings time.

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

Variable definitions

Variable	Value
startWeek <1-5>|last>	Specifies the week of the month (starting on a 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 are counted starting from the first day of the month, not calendar weeks; so, weeks 1-4 would not always apply. Week 5 may not apply in certain years. In that case, summer time start/end falls back to the 'last' option. Years with no Sunday in the fifth week of March For years without a Sunday in the fifth week of March, summer time will start on the last Sunday of March.
<start:DAY>	Specifies the day of the particular month you want recurring daylight savings time to start.
<start:MONTH>	Specifies the month of each year you want recurring daylight savings time to start.
<start:hh:mm>	Specifies the hour and minutes of the particular day you want recurring daylight savings time to start.
endWeek <1-5>|last>	Specifies the week of the month (starting on a 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 are counted starting from the first day of the month, not calendar weeks; so, weeks 1-4 would not always apply. Week 5 may not apply in certain years. In that case,

Variable	Value
	summer time start/end falls back to the 'last' option.
<end:DAY>	Specifies the day of the particular month you want recurring daylight savings time to end.
<end:MONTH>	Specifies the month of each year you want recurring daylight savings time to end.
<end:hh:mm>	Specifies the hour and minute of the particular day you want recurring daylight savings time to end.
offset <1-1440>	Specifies the time in minutes by which you want to change the time when recurring daylight savings begins and ends. The offset is added to the current time when daylight saving time begins and subtracted from the current time when daylight saving time ends. Values range from 1 to 1440 minutes.

Clock configuration

In addition to SNTP time configuration, a clock provides the switch with time information. This clock provides the switch information in the instance that SNTP time is not available.

Use the Clock source command to view and configure the clock.

Clock source command

This command sets the default clock source for the switch.

The syntax for this command is

```
clock source {sntp | sysUpTime}
```

Substitute **{sntp | sysUpTime}** with the clock source selection.

Run this command in Global Configuration command mode.

Custom Autonegotiation Advertisements

Custom Autonegotiation Advertisement (CANA) customizes the capabilities that are advertised. It also controls the capabilities that the Avaya Ethernet Routing Switch 4500 Series advertises as part of the auto negotiation process.

The following sections describe configuring CANA using ACLI:

- Configuring CANA on page 158
- Viewing current auto-negotiation advertisements on page 158
- Viewing hardware capabilities on page 158
- Setting default auto-negotiation-advertisements on page 158
- no auto-negotiation-advertisements command on page 159

Configuring CANA

Use the **auto-negotiation-advertisements** command to configure CANA.

To configure port 5 to advertise the operational mode of 10 Mb/s and full duplex enter the following command:

```
auto-negotiation-advertisements port 5 10-full
```

Viewing current auto-negotiation advertisements

To view the autonegotiation advertisements for the device, enter the following command:

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

Viewing hardware capabilities

To view the available operational modes for the device, enter the following command:

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

Setting default auto-negotiation-advertisements

The **default auto-negotiation-advertisements** command makes a port advertise all auto negotiation capabilities.

The syntax for the **default auto-negotiation-advertisements** command is

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

To set default advertisements for port 5 of the device, enter the following command:

```
default auto-negotiation-advertisements port 5
```

Run the **default auto-negotiation-advertisements** command in Interface Configuration mode.

no auto-negotiation-advertisements command

The **no auto-negotiation-advertisements** command makes a port silent.

The syntax for the **no auto-negotiation-advertisements** command is

```
no auto-negotiation-advertisements [port <portlist>]
```

Run the **no auto-negotiation-advertisements** command in Interface Configuration mode.

Connecting to Another Switch

Use ACLI to communicate with another switch while maintaining the current switch connection, by running the **ping** and **telnet** commands.

ping command

Use the **ping** command to determine whether communication with another switch can be established.

The ping command tests the network connection to another network device by sending an Internet Control Message Protocol (ICMP) packet from the switch to the target device.

Important:
You must set the local IP address before you issue the ping command.

The syntax for this command is

```
ping <ipv6_address | dns_host_name> [datasize <64-4096>] [{count
<1-9999>} | continuous] [{timeout | -t} <1-120>] [interval <1-60>]
[debug]
```

Substitute **<ipv6_address | dns_host_name>** with either the IPv6 address or the DNS host name of the unit to test.

Run this command in User EXEC command mode or any of the other command modes.

Table 71: ping parameters

Parameter	Description
ipv6_address | dns_host_name	IPv6 address or DNS host name of the unit to test.
datasize <64–4096>	Specify the size of the ICMP packet to be sent. The data size range is from 64 to 4096 bytes.

Parameter	Description
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.
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.

telnet command

Use the **telnet** command to establish communications with another switch during the current ACLI session. Communication can be established to only one external switch at a time using the **telnet** command.

The syntax for this command is

```
telnet <ipv6_address | dns_host_name>
```

Substitute **<ipv6_address | dns_host_name>** with either the IPv6 address or the DNS host name of the unit with which to communicate.

Run this command in User EXEC command mode.

Domain Name Server (DNS) Configuration

Use domain name servers when the switch needs to resolve a domain name (such as avaya.com) to an IP address. Use the following commands to configure the switch domain name servers:

- show ip dns command on page 161
- ip domain-name command on page 161
- no ip domain-name command on page 161
- default ip domain-name command on page 161
- ip name-server command on page 162
- no ip name-server command on page 162

show ip dns command

Use the **show ip dns** command to display DNS-related information. This information includes the default switch domain name and any configured DNS servers.

The syntax for this command is

```
show ip dns
```

Run this command in User EXEC command mode.

ip domain-name command

Use the **ip domain-name** command to set the default DNS domain name for the switch. This default domain name is appended to all DNS queries or commands that do not already contain a DNS domain name.

The syntax for this command is

```
ip domain-name <domain_name>
```

Substitute **<domain_name>** with the default domain name. A domain name is deemed valid if it contains alphanumeric characters and at least one period (.).

Run this command in Global Configuration command mode.

no ip domain-name command

Use the **no ip domain-name** command to clear a previously configured default DNS domain name for the switch.

The syntax for this command is

```
no ip domain-name
```

Run this command in Global Configuration command mode.

default ip domain-name command

Use the **default ip domain-name** command to set the system default switch domain name. Because this default is an empty string, this command has the same effect as the **no ip domain-name** command.

The syntax for this command is:

```
default ip domain-name
```

Run this command in Global Configuration command mode.

ip name-server command

Use the **ip name-server** command to set the domain name servers the switch uses to resolve a domain name to an IP address. A switch can have up to three domain name servers specified for this purpose.

The syntax of this command is

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

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

Table 72: ip name-server parameters on page 162 outlines the parameters for this command.

Table 72: ip name-server parameters

Parameter	Description
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.

Run this command in Global Configuration command mode.

no ip name-server command

Use the **no ip name-server** command to remove domain name servers from the list of servers used by the switch to resolve domain names to an IP address.

The syntax for this command is

```
no ip name-server <ip_address_1> no ip name-server [<ip_address_2>]
no ip name-server [<ip_address_3>]
```

Important:

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

Table 73: no ip name-server parameters on page 163 outlines the parameters for this command.

Table 73: no ip name-server parameters

Parameter	Description
<ip_address_1>	The IP address of the domain name server to remove.
<ip_address_2>	Optional. The IP address of a domain name server to remove from the list of servers used by the switch.
<ip_address_3>	Optional. The IP address of a domain name server to remove from the list of servers used by the switch.

Run this command in Global Configuration command mode.

Serial Security

This feature involves logout event when serial console is pulled out.

The commands for serial security are:

```
4548GT-PWR(config)#serial-security enable
```

- Enable serial security

```
4548GT-PWR(config)#no serial-security enable
```

- Disable serial security

```
4548GT-PWR(config)#default serial-security enable
```

Important:

By default this feature is disabled, the `show serial-security` command displays the status of the serial security.

Following is an example for `show serial-security` command:

```
4548GT-PWR#show serial-security
```

```
Serial security is disabled
```

The following message should be logged during the logout event:

```
I 00:02:39:52 23 #0 Session closed (console cable disconnected),
serial connection, access mode: no security
```

Important:

When loading an ASCII configuration file on switch, removing the console cable does not involve a logout event.

Configuring LLDP using ACLI

You can enable and configure LLDP using ACLI. For more information about LLDP, see Link Layer Discovery Protocol (IEEE 802.1AB) Overview on page 63. This section covers the following commands:

lldp command

The **lldp** command sets the LLDP transmission parameters. The syntax for the **lldp** command is

```
lldp [tx-interval <5-32768>] [tx-hold-multiplier <2-10>] [reinit-
delay <1-10>] [tx-delay <1-8192>] [notification-interval <5-3600>]
[med-fast-start <1-10>]
```

Run the **lldp** command in Global Configuration command mode.

The following table describes the variables for the **lldp** command.

Table 74: lldp command variables

Variables	Description
tx-interval <5-32768>	Set the interval between successive transmission cycles.
tx-hold-multiplier <2-10>	Set the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV.
reinit-delay <1-10>	Set the delay for the reinitialization attempt if the adminStatus is disabled.
tx-delay <1-8192>	Set the minimum delay between successive LLDP frame transmissions.
med-fast-start <1-10>	Set value for med-fast-start.
notification-interval <5-3600>	Set the interval between successive transmissions of LLDP notifications.

lldp port command

The **lldp port** command sets the LLDP port parameters. The syntax for the **lldp port** command is

```
lldp port <portlist> [config notification] [status {rxOnly | txAndRx
| txOnly}]
```

Run the **lldp port** command in Interface Configuration command mode.

The following table describes the variables for the **lldp port** command.

Table 75: lldp port command variables

Variables	Description
port <portlist>	Specify the ports affected by the command.
config notification	Enable notification when new neighbor information is stored or when existing information is removed. The default value is *enabled*.

Variables	Description
status {rxOnly | txAndRx | txOnly}	Set the LLDPU transmit and receive status on the ports. • rxonly: enables LLDPU receive only • txAndRx: enables LLDPU transmit and receive • txOnly: enables LLDPU transmit only

lldp med-network-policies command

The **lldp med-network-policies** command configures LLDP Media Endpoint Devices (MED) policies for switch ports. The syntax for the **lldp med-network-policies** command is

```
lldp med-network-policies [port <portList>] {voice|voice-signaling}
[dscp <0-63>] [priority <0-7>] [tagging {tagged|untagged}] [vlan-id
<0-4094>]
```

Run the **lldp med-network-policies** command in Interface Configuration command mode.

The following table describes the variables for the **lldp med-network-policies** command.

Table 76: lldp med-network-policies command variables

Variable	Value
port <portlist>	Specifies the port or ports on which to configure LLDP MED policies.
voice	Specifies voice network policy. The default value is 46.
voice-signaling	Specifies voice signalling network policy.
dscp <0-63>	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63. The default value is 46.
priority <0-7>	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. Values range from 0–7. The default value is 6.
tagging {tagged | untagged}	Specifies the type of VLAN tagging to apply on the selected switch port or ports.

Variable	Value
	• tagged—uses a tagged VLAN • untagged—uses an untagged VLAN or does not support port-based VLANs. If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.
vlan-id <0-4094>	Specifies the VLAN identifier for the selected port or ports. Values range from 0–4094 (0 is for priority tagged frames). If you select priority tagged frames, the system recognizes only the 802.1p priority level and uses a value of 0 for the VLAN ID of the ingress port.

lldp tx-tlv command

The **`lldp tx-tlv`** command sets the optional Management TLVs to be included in the transmitted LLDPDUs.

The syntax for the **`lldp tx-tlv`** command is:

```
lldp tx-tlv [port <portlist>] [local-mgmt-addr] [port-desc] [sys-cap]
[sys-desc][sys-name]
```

Run the **`lldp tx-tlv`** command in Interface Configuration command mode.

The following table describes the variables for the **`lldp tx-tlv`** command.

Table 77: lldp tx-tlv command variables

Variables	Description
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.
port-desc	The port description TLV This TLV is enabled by default. This TLV is enabled by default.
port <portlist>	Specifies a port or list of ports.
sys-cap	The system capabilities TLV.
sys-desc	The system description TLV. This TLV is enabled by default.
sys-name	The system name TLV. This TLV is enabled by default.

Variables	Description
med	The Media Endpoint Device (MED) for a specific TLV.

lldp tx-tlv dot1 command

The **lldp tx-tlv dot1** command sets the optional IEEE 802.1 organizationally-specifc TLVs to be included in the transmitted LLDPDUs. The syntax for the **lldp tx-tlv dot1** command is

```
(config)#lldp tx-tlv [port <portlist>] dot1 [port-protocol-vlan-id
<vlanlist>] [port-vlan-id ] [protocol-identity < [EAP] [LLDP] [STP]>]
[vlan-name <vlanlist>]
```

The **lldp tx-tlv dot1** command is in the Interface Configuration command mode.

The following table describes the variables for the **lldp tx-tlv dot1** command.

Table 78: lldp tx-tlv dot1 command variables

Variables	Description
port <portlist>	The ports affected by the command.
port-protocol-vlan-id <vlanlist>	The port and protocol VLAN ID TLV.
port-vlan-id	The port VLAN ID TLV.
protocol-identity <[EAP] [LLDP] [STP]>	Protocol Identity TLV
vlan-name <vlanlist>	The VLAN name TLV.

lldp tx-tlv dot3 command

The **lldp tx-tlv dot3** command sets the optional IEEE 802.3 organizationally-specifc TLVs to be included in the transmitted LLDPDUs. The syntax for the **lldp tx-tlv dot3** command is

```
(config-if)#lldp tx-tlv [port <portlist>] dot3 [link-aggregation]
[mac-phy-config-status] [maximum-frame-size][mdi-power-support]
```

Run the **lldp tx-tlv dot3** command in Interface Configuration command mode.

The following table describes the variables for the **lldp tx-tlv dot3** command.

Table 79: lldp tx-tlv dot3 command variables

Variables	Description
port <portlist>	The ports affected by the command.
link-aggregation	The link aggregation TLV.
mac-phy-config-status	The MAC/Phy configuration or status TLV.
maximum-frame-size	Maximum Frame Size TLV.
mdi-power-support	The power via MDI TLV. This TLV is enabled by default.

lldp tx-tlv med command

The **`lldp tx-tlv med`** command sets the optional organizationally specific TLVs for use by MED devices to be included in the transmitted LLDPDUs. The syntax for the **`lldp tx-tlv med`** command is:

```
lldp tx-tlv [port <portlist>] med [med-capabilities] [extendedPSE]
[inventory] [location] [network-policy]
```

The **`lldp tx-tlv med`** command is in the config-if command mode.

The following table lists the variables for the **`lldp tx-tlv med`** command.

Table 80: lldp tx-tlv med command variables

Variables	Description
port <portlist>	specifies the ports affected by the command
med-capabilities	MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted). This TLV is enabled by default.
extendedPSE	Extended PSE TLV This TLV is enabled by default.
inventory	Inventory TLVs This TLV is enabled by default.
location	Location Identification TLV This TLV is enabled by default.
network-policy	Network Policy TLV This TLV is enabled by default.

default lldp command

The **default lldp** command sets the LLDP transmission parameters to their default values. The syntax for the **default lldp** command is

```
default lldp [tx-interval ] [tx-hold-multiplier ] [reinit-delay] [tx-
delay] [notification-interval] [med-fast-start]
```

If no parameters are specified, the **default lldp** sets all parameters to their default parameters.

Run the **default lldp** command in Global Configuration command mode.

The following table describes the variables for the **default lldp** command.

Table 81: default lldp command variables

Variables	Description
tx-interval	Set the retransmit interval to the default value (30).
tx-hold-multiplier	Set the transmission multiplier to the default value (4).
reinit-delay	Set the reinitialize delay to the default value (2).
tx-delay	Set the transmission delay to the default value (2).
notification-interval	Set the notification interval to the default value (5).
med-fast-start	Set the MED fast start repeat count to the default value.

default lldp port command

The **default lldp port** command sets the port parameters to their default values. The syntax for the **default lldp port** command is

```
default lldp port <portlist> [config notification] [status]
```

Run the **default lldp port** command in Interface Configuration command mode.

The following table describes the variables for the **default lldp port** command.

Table 82: default lldp port command variables

Variables	Description
port <portlist>	The ports affected by the command.

Variables	Description
config notification	Set the config notification to its default value (disabled).
status	Set the LLDPU transmit and receive status to the default value (txAndRx).

default lldp med-network-policies command

The **default lldp med-network-policies** command configures LLDP MED policies for switch ports to default values. The syntax for the **default lldp med-network-policies** command is:

```
default lldp med-network-policies [port <portList>] {voice|voice-signaling}
```

Run the **default lldp med-network-policies** command in Interface Configuration command mode.

The following table describes the variables for the **default lldp med-network-policies** command.

Table 83: default lldp med-network-policies command variables

Variable	Value
port <portlist>	Specifies the port or ports on which to configure default LLDP MED policies.
voice	Specifies the default voice network policy. The default value is 46.
voice-signaling	Specifies the default voice signalling network policy.

default lldp tx-tlv command

The **default lldp tx-tlv** command sets the LLDP Management TLVs to their default values. The syntax for the **default lldp tx-tlv** command is

```
default lldp tx-tlv [port <portlist>][port-desc] [sys-name] [sys-desc] [sys-cap] [local-mgmt-addr]
```

Run the **default lldp tx-tlv** command in Interface Configuration command mode.

The following table describes the variables for the **default lldp tx-tlv** command.

Table 84: default lldp tx-tlv command variables

Variables	Description
port <portlist>	The ports affected by the command.
port-desc	The port description TLV. This TLV is enabled by default.
sys-name	The system name TLV. This TLV is enabled by default.
sys-desc	The system description TLV. This TLV is enabled by default.
sys-cap	The system capabilities TLV (default value is false: not included).
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.

default lldp tx-tlv dot1 command

The **`default lldp tx-tlv dot1`** command sets the optional IEEE 802.1 organizationally-specifc TLVs to their default values. The syntax for the **`default lldp tx-tlv dot1`** command is

```
default lldp tx-tlv [port <portlist>] dot1 [port-vlan-id] [vlan-
name ] [port-protocol-vlan-id] [protocol-identity [EAP] [LLDP]
[STP] ]
```

Run the **`default lldp tx-tlv dot1`** command in Interface Configuration command mode.

The following table describes the variables for the **`default lldp tx-tlv dot1`** command.

Table 85: default lldp tx-tlv dot1 command variables

Variables	Description
port <portlist>	The ports affected by the command.
port-vlan-id	The port VLAN ID TLV (default value is false: not included).
vlan-name	The VLAN Name TLV (default value is none).
port-protocol-vlan-id	The port and protocol VLAN ID TLV (default value is none).
protocol-identity [EAP] [LLDP] [STP]	The protocol identity TLV (default value is none).

default lldp tx-tlv dot3 command

The **`default lldp tx-tlv dot3`** command sets the optional IEEE 802.3 organizationally-specifc TLVs to their default values. The syntax for the **`default lldp tx-tlv dot3`** command is

```
default lldp tx-tlv [port <portlist>] dot3 [mac-phy-config-status]
[mdi-power-support] [link-aggregation][maximum-frame-size]
```

Run the **`default lldp tx-tlv dot3`** command in Interface Configuration command mode.

The following table describes the variables for the **`default lldp tx-tlv dot3`** command.

Table 86: default lldp tx-tlv dot3 command variables

Variables	Description
port <portlist>	The ports affected by the command.
mac-phy-config-status	The MAC/Phy Configuration/Status TLV (default value is false: not included).
mdi-power-support	The power via MDI TLV. This TLV is enabled by default.
link-aggregation	The link aggregation TLV (default value is false: not included).
maximum-frame-size	The maximum frame size TLV (default value is false: not included).

default lldp tx-tlv med command

The **`default lldp tx-tlv med`** command sets default values for the optional organizationally specific TLVs for use by MED devices to be included in the transmitted LLDPDUs. The syntax for the **`default lldp tx-tlv med`** command is:

```
default lldp tx-tlv [port <portlist>] med [med-capabilities]
[extendedPSE] [inventory] [location] [network-policy]
```

The **`default lldp tx-tlv med`** command is in the config-if command mode.

The following table lists the variables for the **`default lldp tx-tlv med`** command.

Table 87: default lldp tx-tlv med command variables

Variables	Description
port <portlist>	specifies the ports affected by the command
med-capabilities	MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted). This TLV is enabled by default.
extendedPSE	Extended PSE TLV This TLV is enabled by default.
inventory	Inventory TLVs This TLV is enabled by default.
location	Location Identification TLV This TLV is enabled by default.
network-policy	Network Policy TLV This TLV is enabled by default.

no lldp port command

The **no lldp port** command disables LLDP features on the port. The syntax for the **no lldp port** command is

```
no lldp [port <portlist>] [config notification] [status]
```

Run the **no lldp port** command in Interface Configuration command mode.

no lldp med-network-policies command

The **no lldp med-network-policies** command disables LLDP MED policies for switch ports. The syntax for the **no lldp med-network-policies** command is

```
no lldp med-network-policies [port <portList>] {voice|voice-
signaling}
```

Run the **no lldp med-network-policies** command in Interface Configuration command mode.

The following table describes the variables for the **no lldp med-network-policies** command.

Table 88: no lldp med-network-policies command variables

Variable	Value
port <portlist>	Specifies the port or ports on which to disable LLDP MED policies.
voice	Specifies the voice network policy to disable.
voice-signaling	Specifies the voice signalling network policy to disable.

no lldp tx-tlv command

The **no lldp tx-tlv** command specifies the optional Management TLVs not to include in the transmitted LLDPDUs. The syntax for the **no lldp tx-tlv** command is

```
no lldp tx-tlv [port <portlist>] [port-desc] [sys-name] [sys-desc]
[sys-cap] [local-mgmt-addr]
```

Run the **no lldp tx-tlv** command in Interface Configuration command mode.

The following table describes the variables for the **no lldp tx-tlv** command.

Table 89: default lldp tx-tlv command variables

Variables	Description
port <portlist>	The ports affected by the command.
port-desc	The port description TLV. This TLV is enabled by default.
sys-name	The system name TLV. This TLV is enabled by default.
sys-desc	The system description TLV. This TLV is enabled by default.
sys-cap	The system capabilities TLV (default value is false: not included).
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.

no lldp tx-tlv dot1 command

The **no lldp tx-tlv dot1** command specifies the optional IEEE 802.1 TLVs not to include in the transmitted LLDPDUs. The syntax for the **no lldp tx-tlv dot1** command is

```
no lldp tx-tlv [port <portlist>] dot1 [port-vlan-id] [vlan-name]
[port-protocol-vlan-id] [protocol-identity [EAP] [LLDP] [STP] ]
```

Run the **no lldp tx-tlv dot1** command in Interface Configuration command mode.

no lldp tx-tlv dot3 command

The **no lldp tx-tlv dot3** command specifies the optional IEEE 802.3 TLVs not to include in the transmitted LLDPDUs. The syntax for the **no lldp tx-tlv dot3** command is

```
no lldp tx-tlv [port <portlist>] dot3 [mac-phy-config-status] [mdi-
power-support] [link-aggregation][maximum-frame-size]
```

Run the **no lldp tx-tlv dot3** command in Interface Configuration command mode.

show lldp command

The **show lldp** command displays the LLDP parameters. The syntax for the **show lldp** command is

```
show lldp [local-sys-data {dot1 | dot3 | detail | med }] [mgmt-sys-
data] [rx-stats] [tx-stats] [stats] [pdu-tlv-size] [tx-tlv {dot1 |
dot3 | med }] [neighbor { dot1 [vlan-names | protocol-id] } | [dot3]
| [detail] | med [capabilities | extended-power | inventory |
location | network-policy]} [neighbor-mgmt-addr]
```

Run the **show lldp** command in Privileged EXEC command mode.

The following table describes the **show lldp** command variables.

Table 90: show lldp command variables

Variables	Description
local-sys-data {dot1 | dot3 | detail | med}	The organizationally-specific TLV properties on the local switch: • dot1: displays the 802.1 TLV properties • dot3: displays the 802.3 TLV properties • detail: displays all organizationally specific TLV properties • med: displays all med specific TLV properties To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.
mgmt-sys-data	The local management system data.

Variables	Description
neighbor { dot1 [vlan-names | protocol-id] } | [dot3] [detail] | med [capabilities | extended-power | inventory | location | network-policy]	The neighbor TLVs: • dot1: displays 802.1 TLVs: - vlan-names: VLAN Name TLV - protocol-id: Protocol Identity TLV • dot3: displays 802.3 TLVs • detail: displays all TLVs • med: displays MED TLVs • capabilities: Displays Capabilities TLVs • extended-power: Displays extended power TLV • inventory: Displays Inventory TLVs • location: Displays Location TLV • network-policy: Displays Network Policy TLV
neighbor-mgmt-addr	Display 802.1ab neighbors management addresses.
pdu-tlv-size	The different TLV sizes and the number of TLVs in an LLDPDU.
port	Port list.
rx-stats	The LLDP receive statistics for the local system.
stats	The LLDP table statistics for the remote system.
tx-stats	The LLDP transmit statistics for the local system.
tx-tlv {dot1 | dot3 | med}	Display which TLVs are transmitted from the local switch in LLDPDUs: • dot1: displays status for 802.1 TLVs • dot3: displays status for 802.3 TLVs • med: displays status for med TLVs To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.

Job aid: show lldp mgmt-sys-data command

The following figure displays sample output for the **`show lldp`** command with the *mgmt-sys-data* variable.

```
4526GTX-PWR#show lldp mgmt-sys-data
-------------------------------------------------------------------------------
                              LLDP mgmt-sys-data
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
MgmtAddr                           MgmtIfId MgmtAddrOID
-------------------------------------------------------------------------------
IPv4  10.100.120.21                0        1.3.6.1.4.1.45.3.71.6
IPv6  2120::30                     0        1.3.6.1.4.1.45.3.71.6
-------------------------------------------------------------------------------
4526GTX-PWR#
```

show lldp port command

The **show lldp port** command displays the LLDP port parameters.

The syntax for the **show lldp port** command is:

```
show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 |
detail | med }][rx-stats] [tx-stats] [pdu-tlv-size] [tx-tlv {dot1 |
dot3 | med | vendor-specific}] [neighbor-mgmt-addr] [neighbor {dot1 |
dot3 | detail | med }
```

Run the **show lldp port** command in Privileged EXEC command mode.

Table 91: show lldp port command variables

Variables	Description
local-sys-data {dot1 | dot3 | detail | med }	The organizationally-specific TLV properties on the local switch: • dot1: displays the 802.1 TLV properties • dot3: displays the 802.3 TLV properties • detail: displays all organizationally specific TLV properties • med: displays all med specific TLV properties To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.
rx-stats	The LLDP receive statistics for the local port.
tx-stats	The LLDP transmit statistics for the local port.
pdu-tlv-size	The different TLV sizes and the number of TLVs in an LLDPDU.
port <portlist> | all	Specifies an individual port, a list of specific ports, or all ports on the switch.
tx-tlv {dot1 | dot3 | med | vendor-specific}	Display which TLVs are transmitted from the local port in LLDPDUs:

Variables	Description
	• dot1: displays status for 802.1 TLVs • dot3: displays status for 802.3 TLVs • med: displays status for med TLVs • vendor-specific:displays vendor specific TLV information To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.
neighbor {dot1 | dot3 | detail | med }	The port neighbor TLVs: • dot1: displays 802.1 TLVs: • dot3: displays 802.3 TLVs • detail: displays all TLVs. • med: displays MED TLVs • vendor-specific:displays vendor specific TLV information
[neighbor-mgmt-addr]	The port neighbor LLDP management address. The switch supports IPv4 and IPv6 management addresses.

Job aid: show lldp port command output

The following figure displays sample output for the **show lldp port** command with the *tx-tlv* variable.

```
4524GT-PWR#show lldp port 1-5 tx-tlv
-------------------------------------------------------------------------------
                              LLDP port tlvs
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Port   PortDesc SysName  SysDesc  SysCap   MgmtAddr
-------------------------------------------------------------------------------
1       false    false    false    true     true
2       false    false    false    true     false
3       false    false    false    true     false
4       false    false    false    true     false
5       false    false    false    true     false
-------------------------------------------------------------------------------
4524GT-PWR#
```

show lldp med-network-policies command

The **show lldp med-network-policies** command displays LLDP MED policy information for switch ports. The syntax for the **show lldp med-network-policies** command is:

```
show lldp med-network-policies [port <portList>] {voice|voice-
signaling}
```

Run the **show lldp med-network-policies** command in Privileged EXEC command mode.

The following table describes the variables for the **show lldp med-network-policies** command.

Table 92: show lldp med-network-policies command variables

Variable	Value
port <portlist>	Specifies the port or ports for which to display LLDP MED policy information.
voice	Displays the voice network policy for which to display information. The default value is 46.
voice-signaling	Specifies the voice signalling network policy to disable.
Note: The default DSCP value is 46 and the default priority value is 6.	

Configuring the PoE conservation level request TLV using ACLI

Use this procedure to request a specific power conservation level for an Avaya IP phone connected to a switch port.

Prerequisites

Log on to the Interface Configuration mode in ACLI.

Procedure steps

1. Configure PoE conservation level TLVs for connected Avaya IP phones by using the following command:

   ```
   lldp [port <portList>] vendor-specific avaya poe-
   conservation-request-level <0-255>
   ```

2. Set PoE conservation level TLVs for connected Avaya IP phones to the default value by using the following command:

   ```
   default [port <portList>] lldp vendor-specific avaya poe-
   conservation-request-level
   ```

Important:

Only Ethernet ports on switches that support PoE can request a specific power conservation level for an Avaya IP phone.

Variable definitions

Variable	Value
<0-255>	Specifies the power conservation level to request for a vendor specific PD. Values range from 0 to 255. With the default value of 0, the switch does not request a power conservation level for an Avaya IP phone connected to the port.
<portList>	Specifies a port or list of ports.

Viewing the switch PoE conservation level request TLV configuration using ACLI

Use this procedure to display Poe conservation level request configuration for local switch ports.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display the PoE conservation level request configuration for one or more switch ports by using the following command:

```
show lldp [port <portlist>] vendor-specific avaya poe-
conservation-request-level
```

Variable definitions

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

Job aid: show lldp vendor-specific avaya poe-conservation-request-level command output

The following figure displays sample output for the **`show lldp vendor-specific avaya poe-conservation-request-level`** command.

```
4524GT-PWR#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
4524GT-PWR(config)#interface fastethernet 1,2
4524GT-PWR(config-if)#show lldp vendor-specific avaya poe-conservation-request-level
-------------------------------------------------------------------------------
              LLDP vendor-specific Avaya POE Request Conservation Level
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
      Unit/        POE Request
      Port           Level
-------------------------------------------------------------------------------
      1              2
      2              45
4524GT-PWR(config-if)#
```

Viewing PoE conservation level support TLV information using ACLI

Use this procedure to display PoE conservation level information received on switch ports from an Avaya IP phone.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display the received PoE conservation level information for one or more switch ports by using the following command:

`show lldp [port <portlist>] neighbor vendor-specific avaya poe-conservation`

Variable definitions

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

Configuring the switch call server IP address TLV using ACLI

Use this procedure to define the local call server IP addresses that switch ports advertise to Avaya IP phones.

You can define IP addresses for a maximum of 8 local call servers.

Important:
The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Define the local call server IPv4 addresses the switch advertises to Avaya IP phones by using the following command:

```
lldp vendor-specific avaya call-server [<1-8>] <A.B.C.D>
[[<1-8>] <A.B.C.D>] [[<1-8>] <A.B.C.D>]
```

2. Delete call server IPv4 addresses configured on the switch by using the following command:

```
default lldp vendor-specific avaya call-server <1-8>
```

Variable definitions

Variable	Value
<1-8>	Specifies the call server number. **Note:** When you advertise the IPv4 address of call server 1 only, you do not have to enter a call server number before you enter the IP address.
<A.B.C.D>	Specifies the call server IPv4 address.

Viewing the switch call server IP address TLV configuration using ACLI

Use this procedure to display information about the defined local call server IP address that switch ports advertise to connected Avaya IP phones.

The switch supports a maximum of 8 local call servers.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display call server TLV configuration information for the local switch by using the following command:

```
show lldp vendor-specific avaya call-server
```

Job aid: show lldp vendor-specific call-server command output

The following figure displays sample output for the **`show lldp vendor-specific avaya call-server`** command.

```
4524GT-PWR(config)#sho lldp vendor-specific avaya call-server
--------------------------------------------------------------------------------
                     LLDP Avaya Call Servers IP addresses
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
   Avaya Configured Call Server 1: 10.10.10.4
   Avaya Configured Call Server 2: 10.10.10.1
   Avaya Configured Call Server 3: 10.10.10.2
--------------------------------------------------------------------------------
4524GT-PWR(config)#
```

Viewing Avaya IP phone call server IP address TLV information using ACLI

Use this procedure to display call server IP address information received on switch ports from an Avaya IP phone.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display call server TLV configuration information received on specific switch ports from connected Avaya IP phones by using the following command:

```
show lldp [port <portlist>] neighbor vendor-specific avaya
call-server
```

Variable definitions

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

Configuring the switch file server IP address TLV using ACLI

Use this procedure to define the local file server IP addresses that switch ports advertise to Avaya IP phones.

You can define IP addresses for a maximum of 4 local file servers.

Note:

If your Avaya IP Handset uses SIP, 802.1AB (LLDP) TLVs do not provide all information for the IP Phone. You must specify a file server IP address TLV so the IP phone can download the SIP configuration information, because the IP Phone retrieves information related to the SIP domain, port number and transport protocol from the file server.

Important:
The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

1. Enable file server IPv4 address advertisement to Avaya IP phones by using the following command:

```
lldp vendor-specific avaya file-server [<1-4>] <A.B.C.D>
[[<1-4>] <A.B.C.D>] [[<1-4>] <A.B.C.D>]
```

2. Delete file server IPv4 addresses configured on the switch by using the following command:

```
default lldp vendor-specific avaya file-server <1-4>
```

Variable definitions

Variable	Value
<1-4>	Specifies the file server number. **Note:** When you advertise the IPv4 address of file server 1 only, you do not have to enter a file server number before you enter the IP address.
<A.B.C.D>	Specifies the file server IPv4 address.

Viewing the switch file server IP address TLV configuration using ACLI

Use this procedure to display information about the defined local file server IP address that switch ports advertise to connected Avaya IP phones.

You can define IP addresses for a maximum of 4 local file servers.

Important:
The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

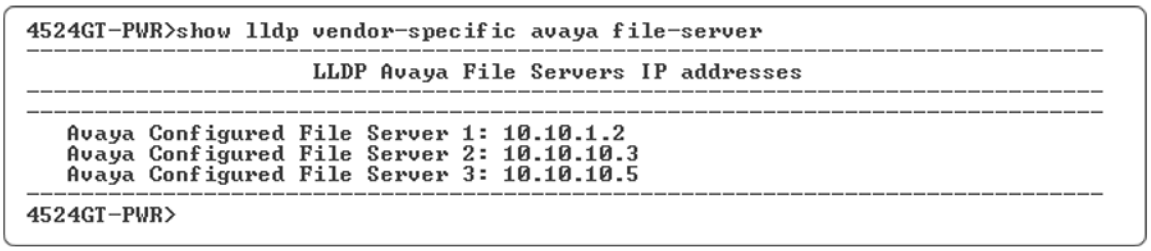
Procedure steps

Display file server TLV configuration information for the switch by using the following command:

```
show lldp vendor-specific avaya file-server
```

Job aid: show lldp vendor-specific file-server command output

The following figure displays sample output for the show lldp vendor-specific avaya file-server command.



```
4524GT-PWR>show lldp vendor-specific avaya file-server
--------------------------------------------------------------------------------
                     LLDP Avaya File Servers IP addresses
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
   Avaya Configured File Server 1: 10.10.1.2
   Avaya Configured File Server 2: 10.10.10.3
   Avaya Configured File Server 3: 10.10.10.5
--------------------------------------------------------------------------------
4524GT-PWR>
```

Viewing Avaya IP phone file server IP address TLV information using ACLI

Use this procedure to display information about file server IP address received on switch ports from Avaya IP phones.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display file server advertisement configuration information received on specific switch ports from connected Avaya IP phones by using the following command:

```
show lldp [port <portlist>] neighbor vendor-specific avaya
file-server
```

Variable definitions

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

Configuring the 802.1Q framing TLV using ACLI

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Prerequisites

- Enable LLDP MED capabilities.
- Enable LLDP MED network policies.
- Log on to the Interface Configuration mode in ACLI.

Procedure steps

1. Configure the Layer 2 frame tagging mode by using the following command:

   ```
   lldp [port <portlist>] vendor-specific avaya dot1q-framing
   [tagged | non-tagged | auto]
   ```

2. Set the Layer 2 frame tagging mode to default by using the following command:

   ```
   default lldp [port <portlist>] vendor-specific avaya dot1q-
   framing
   ```

Variable definitions

Variable	Value
<portlist>	Specifies a port or list of ports.
[tagged | non-tagged | auto]	Specifies the frame tagging mode. Values include: • tagged—frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • non-tagged—frames are not tagged with 802.1Q priority. • auto—an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. The default tagging mode is auto.

Viewing the switch 802.1Q Framing TLV configuration using ACLI

Use this procedure to display the configured Layer 2 frame tagging mode for switch ports.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display the configured Layer 2 frame tagging mode for one or more switch ports by using the following command:

```
show lldp [port <portlist>] vendor-specific avaya dot1q-framing
```

Variable definitions

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

Job aid: show lldp vendor-specific avaya dot1q-framing command output

The following figure displays sample output for the show lldp vendor-specific avaya dot1q-framing command.

```
4524GT-PWR#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
4524GT-PWR(config)#interface fastethernet 1-10
4524GT-PWR(config-if)#show lldp vendor-specific avaya dot1q-framing
-------------------------------------------------------------------------------
                   LLDP vendor-specific Avaya 802.1Q Framing
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
      Unit/         Framing
      Port        Tagging Mode
-------------------------------------------------------------------------------
      1             tagged
      2             tagged
      3             tagged
      4             tagged
      5             tagged
      6             non-tagged
      7             auto
      8             non-tagged
      9             auto
      10            auto
4524GT-PWR(config-if)#
```

Viewing Avaya IP phone 802.1Q Framing TLV information using ACLI

Use this procedure to display Layer 2 frame tagging mode information received on switch ports from connected Avaya IP phones.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display the received Layer 2 frame tagging mode information for one or more switch ports by using the following command:

```
show lldp [port <portlist>] neighbor vendor-specific avaya
dot1q-framing
```

Variable definitions

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

Enabling Avaya TLV transmit flags using ACLI

Use this procedure to enable the transmission of optional proprietary Avaya TLVs from switch ports to Avaya IP phones.

Important:
The switch transmits configured Avaya TLVs only on ports with the TLV transmit flag enabled.

Prerequisites

Log on to the Interface Configuration mode in ACLI.

Procedure steps

Select the Avaya TLVs that the switch transmits by using the following command:

```
[default] lldp tx-tlv [port <portList>] vendor-specific avaya
{[poe-conservation] [call-server] [file-server] [dot1q-
framing]}
```

Variable definitions

Variable	Value
call-server	Enables the call server TLV transmit flag.
default	Sets the TLV transmit flag to the default value of true (enabled).
dot1q-framing	Enables the Layer 2 priority tagging TLV transmit flag.

Variable	Value
file-server	Enables the file server TLV transmit flag.
poe-conservation	Enables the PoE conservation request TLV transmit flag.
<portList>	Specifies a port or list of ports.

Disabling Avaya TLV transmit flags using ACLI

Use this procedure to disable the transmission of optional proprietary Avaya TLVs from switch ports to Avaya IP phones.

The switch transmits configured Avaya TLVs only on ports with the TLV transmit flag enabled.

Prerequisites

Log on to the Interface Configuration mode in ACLI.

Procedure steps

Disable Avaya TLVs that the switch transmits by using the following command:

```
no lldp tx-tlv [port <portList>] vendor-specific avaya {[poe-conservation] [call-server] [file-server] [dot1q-framing]}
```

Variable definitions

Variable	Value
call-server	Disables the call server TLV transmit flag.
dot1q-framing	Disables the Layer 2 priority tagging TLV transmit flag.
file-server	Disables the file server TLV transmit flag.
poe-conservation	Disables the PoE conservation request TLV transmit flag.
<portList>	Specifies a port or list of ports.

Viewing the Avaya TLV transmit flag status using ACLI

Use this procedure to display the status of transmit flags for switch ports on which Avaya IP phone support TLVs are configured.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display Avaya TLV transmit flag configuration information for one or more switch ports by using the following command in the Interface Configuration mode for one or more ports:

```
show lldp [port <portlist>] tx-tlv vendor-specific avaya
```

Variable definitions

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

Job aid: show lldp tx-tlv vendor-specific avaya command output

The following figure displays sample output for the **show lldp tx-tlv vendor-specific avaya** command.

```
4524GT-PWR#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
4524GT-PWR(config)#interface fastethernet 1-8
4524GT-PWR(config-if)#show lldp tx-tlv vendor-specific avaya
-------------------------------------------------------------------------------
                 LLDP port Avaya Vendor-Specific TLVs
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
      Unit/    POE Conservation   Call-Server   File-Server Dot1Q-Framing
      Port        Request
-------------------------------------------------------------------------------
      1           false          true          false          true
      2           true           true          true           true
      3           false          true          false          true
      4           true           true          true           true
      5           true           true          true           true
      6           true           true          true           true
      7           false          true          false          true
      8           true           true          true           true
4524GT-PWR(config-if)#
```

Viewing Avaya IP phone IP TLV configuration information using ACLI

Use this procedure to display IP address configuration information received on switch ports from connected Avaya IP phones.

Prerequisites

Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Display the received IP address configuration information for one or more switch ports by using the following command:

```
show lldp [port <portlist>] neighbor vendor-specific avaya
phone-ip
```

Variable definitions

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

LLDP configuration example

By default, LLDP is enabled for Tx and Rx on all switch ports. The default value for the LLDP Tx interval is 30 seconds (LLDPDUs are sent at 30 seconds). With the default settings, only the mandatory TLVs are sent, but the switch can receive any LLDP Core, DOT1, DOT3 TLV, or Med-capabilities TLV from its peers.

The following figure shows an example of LLDP configuration. For this example, the router is connected to the Avaya Ethernet Routing Switch 4500 Series port 1 and the IP Phone uses port 13

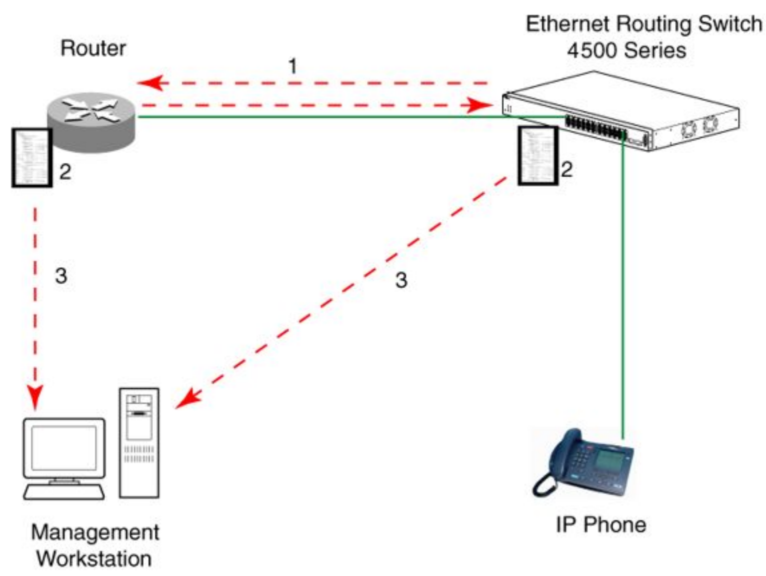


Figure 13: LLDP configuration example

To configure the example shown in the preceding figure, you must perform the following tasks:

1. Modify the default LLDP Tx interval from (the default 30 second value) to 60 seconds.

   Note that if any modification is detected in the LLDP local-sys-data before the Tx interval expires, an LLDPDU is immediately sent on all active links to update the peers neighbor tables.

2. Enable the Port Description TLV for transmission. (contains the description of the LLPD sending port)
3. Enable the System Name TLV for transmission. (contains the name of the LLDP device)
4. Enable the System Description TLV for transmission. (contains the description of the LLDP device)
5. Enable the System Capabilities TLV for transmission. (contains the capabilities of the LLDP device)
6. Enable the Management Address TLV for transmission. (contains the management address of the LLDP device)
7. Enable the Port VLAN ID TLV for transmission. (contains the PVID of the LLDP sending port)
8. Enable the Port And Protocol VLAN ID TLV for transmission. (indicates the Port and Protocol VLANs to which the LLDP sending port belongs to).
9. Enable the VLAN Name TLV for transmission. (indicates the names of the VLANs to which the LLDP sending port belongs to)

10. Enable the Protocol Identity TLV for transmission. (indicates the supported protocols by the LLDP sending port)
11. Enable the MAC/PHY Configuration/Status TLV for transmission. (indicates the IEEE 802.3 duplex and bitrate capabilities and settings of the LLDP sending port)
12. Enable the Power Via MDI TLV for transmission. (indicates the MDI power support capabilities of the LLDP sending port)
13. Enable the Link Aggregation TLV for transmission. (indicates the link aggregation capability and status of the LLDP sending port)
14. Enable the Maximum Frame Size TLV for transmission. (indicates the maximum frame size that can be handled by the LLDP sending port)
15. Enable the Location Identification TLV for transmission. (indicates the physical location of the LLDP sending port; three coordinate sets are available to configure and send)
16. Enable the Extended Power-via-MDI TLV for transmission. (provides detailed informations regarding the PoE parameters of the LLDP sending device)
17. Enable the Inventory – Hardware Revision TLV for transmission. (indicates the hardware revision of the LLDP sending device)
18. Enable the Inventory – Firmware Revision TLV for transmission. (indicates the firmware revision of the LLDP sending device)
19. Enable the Inventory – Software Revision TLV for transmission. (indicates the software revision of the LLDP sending device)
20. Enable the Inventory – Serial Number TLV for transmission. (indicates the serial number of the LLDP sending device)
21. Enable the Inventory – Manufacturer Name TLV for transmission. (indicates the manufacturer name of the LLDP sending device)
22. Enable the Inventory – Model Name TLV for transmission. (indicates the model name of the LLDP sending device)
23. Configure the location information for the LLDP-MED Location Identification TLV. (There are three coordinate sets available for location advertisement.)
24. Enable the LLDP-MED Capabilities TLV for transmission (indicates the supported LLDP-MED TLVs and the LLDP-MED device type of the LLDP sending device)

Detailed configuration commands

The following section describes the detailed ACLI commands required to carry out the configuration depicted by Figure 13: LLDP configuration example on page 193

Modifying the default LLDP Tx interval

Enter configuration commands, one for each line. End with CNTL/Z.

```
4548GT-PWR-PWR>enable
4548GT-PWR#configure terminal
4548GT-PWR(config)#lldp tx-interval 60
```

Checking the new LLDP global settings

```
4548GT-PWR(config)#show lldp
```

```
802.1ab configuration:
----------------------------------------
TxInterval:60
TxHoldMultiplier:4
RxInitDelay:2
TxDelay:2
NotificationInterval:5
MedFastStartRepeatCount:4
```

Enabling all LLDP Core TLVs for transmission on the router and IP Phone ports

```
4548GT-PWR(config)#interface fastEthernet 1/13
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 port-desc
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 sys-name
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 sys-desc
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 sys-cap
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 local-mgmt-addr
```

Checking the LLDP settings of the router and IP Phone ports

The following represents screen output for the **show lldp port 1/13 tx-tlv** command:

```
4548GT-PWR(config-if)#show lldp port 1/13 tx-tlv
```

LLDP port tlvs

Port	PortDesc	SysName	SysDesc	SysCap	MgmtAddr
1	true	true	true	true	true
13	true	true	true	true	true

Enabling all LLDP DOT1 TLVs for transmission on the router and IP Phone ports

```
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot1 port-vlan-id
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot1 port-protocol-vlan-
id
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot1 vlan-name
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot1 protocol-identity
EAP LLDP STP
```

Checking the LLDP settings of the router and IP Phone ports

The following represents screen output for the **show lldp port 1/13 tx-tlv dot1** command:

```
4548GT-PWR(config-if)#show lldp port 1/13 tx-tlv dot1

                          LLDP dot1 port tlvs

 Dot1 protocols: STP,EAP,LLDP

 Port  PortVlanId  VlanNameList  PortProtocol   Protocol
                                 VlanId         Identity

 13    true        1,3,5,7,9,11  1,3,5,7,9,117  EAP,LLDP
                   7-118         -118
```

Enabling all LLDP DOT3 TLVs for transmission on the router and IP Phone ports

```
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot3 mac-phy-config-
status
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot3 mdi-power-support
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot3 link-aggregation
4548GT-PWR(config-if)#lldp tx-tlv port 1/13 dot3 maximum-frame-size
```

Checking the LLDP settings of the router and IP Phone ports

The following represents screen output for the **show lldp port 1/13 tx-tlv dot3** command:

```
4548GT-PWR(config-if)#show lldp port 1/13 tx-tlv dot3
```

LLDP port dot3 tlvs

Port	MacPhy ConfigStatus	MdiPower Support	Link Aggregation	MaxFrameSize
1	true	true	true	true
13	true	true	true	true

Enabling all LLDP MED TLVs for transmission on the router and IP Phone ports

The first three commands are required to configure the location identification for the LLDP-MED Location Identification TLV.

```
4550T (config-if)#lldp location-identification civic-address
country-code US city Boston street Orlando
4550T (config-if)#lldp location-identification coordinate-base
altitude 234 meters datum WGS84
4550T (config-if)#lldp location-identification ecs-elin 1234567890
4550T (config-if)#lldp tx-tlv med port 12,13 med-capabilities
4550T (config-if)#lldp tx-tlv med port 12,13 network-policy
4550T (config-if)#lldp tx-tlv med port 12,13 location
4550T (config-if)#lldp tx-tlv med port 12,13 extendedPSE
4550T (config-if)#lldp tx-tlv med port 12,13 inventory
```

Checking the new LLDP settings of the router and IP Phone ports

The following represents screen output for the **show lldp tx-tlv med** command:

```
4550T (config-if)#show lldp tx-tlv med
```

LLDP port med tlvs

Port	Med Capabiliti es	Network Policy	Location	Extended PSE	Inventory
12	true	true	true	true	true
13	true	true	true	true	true

MED TLVs are transmitted only if Med-Capabilities TLV is transmitted

Asset ID string configuration using ACLI

This section describes the procedures you can perform to configure an asset ID for the switch or stack using ACLI commands.

Configuring Asset ID string

Perform this procedure to configure asset ID of a switch or stack.

Prerequisites

Log on to Global configuration mode.

Procedure steps

1. To configure asset ID enter the following command:

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

2. To verify the asset ID settings enter the following command:

   `show system`

Variable definitions

Use the data in the following table to complete the command in this procedure.

Variable	Value
Stack	Sets the Asset ID of the stack
Unit	Sets the Asset ID of a specific unit
WORD	Sets the Asset ID of the unit on which it is the console

Job aid

Use the following commands to view the configured Asset ID.

- `show system`
- `show sys-info`
- `show tech`
- `show system verbose`

Disabling asset ID string

Perform this procedure to disable the asset ID string.

Prerequisites

Log on to the Global configuration mode in ACLI.

Procedure steps

1. To disable the asset ID string enter the following command:

   `no asset-id [ stack | unit <1-8> | <cr> ]`

2. To verify the asset ID string settings enter the following command:

   `show system`

Variable definitions

Use the data in the following table to complete this procedure.

Variable	Value
Stack	Sets the Asset ID of the stack
Unit <1-8>	Sets the Asset ID for specified unit in the stack. Unit number: 1–8

Setting the asset ID string to default

Perform this procedure to set the asset ID string to default mode.

Prerequisites

Log on to Global configuration mode.

Procedure steps

1. To set the asset ID string to default enter the following command:

   `default asset-id [ stack | unit <1-8> | <cr> ]`
2. To verify the asset ID string settings enter the following command:

   `show system`

Variable definitions

Use the data in the following table to complete this procedure.

Variable	Value
Stack	Sets the default Asset ID of the stack
Unit <1-8>	Sets the default Asset ID for specified unit Unit number: 1–8

AES configuration using ACLI

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

Configuring global AES using ACLI

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

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

Configure global AES by using the following command:

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

Variable definitions

The following table defines optional parameters that you can enter with the **`[no] [default] energy-saver [enable] [efficiency-mode] [poe-power-saving]`** 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.
`[no]`	Disables AES efficiency mode, POE power saving, or AES globally.
`poe-power-saving`	Enables POE power saving.

Variable	Value
	Important: You must disable AES globally before you can modify POE power saving.

Configuring port-based AES using ACLI

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

Prerequisites

- Disable AES globally.
- Log on to the Interface Configuration mode in ACLI.

Procedure steps

Configure port-based AES by using the following command:

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

Variable definitions

The following table defines optional parameters that you enter after the **`[default] [no] energy-saver <enable> [port <portlist> enable]`** command.

Variable	Value
`<enable>`	Enables AES for the accessed port.
`[no]`	Disables AES for the accessed port, an alternate port, or list of ports.
`port <portlist> enable`	Enables AES for a port or list of ports.

Activating or deactivating AES manually using ACLI

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

Prerequisites

- Disable AES globally.
- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

1. Activate AES by using the following command:

   ```
   energy-saver activate
   ```

2. Deactivate AES by using the following command:

   ```
   energy-saver deactivate
   ```

Configuring AES scheduling using ACLI

Use the following 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.

Prerequisites

- Log on to the Global Configuration mode in ACLI.
- Disable AES globally.

Procedure steps

Configure AES scheduling by using the following command:

```
energy-saver schedule {weekday|weekend|monday|tuesday |
wednesday|thursday|friday|saturday|sunday} <hh:mm> {activate|
deactivate}
```

Variable definitions

The following table defines parameters that you can enter with the **energy-saver schedule {weekday|weekend|monday|tuesday |wednesday|thursday|friday|saturday| sunday} <hh:mm> {activate|deactivate}** command.

Variable	Value
<activate>	Specifies the AES on time.
<deactivate>	Specifies the AES off time.
monday|tuesday|wednesday | thursday|friday|saturday| sunday	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.

Disabling AES scheduling using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI.
- Disable AES globally.

Procedure steps

Configure AES scheduling by using the following command:

```
no energy-saver schedule
```

Variable definitions

The following table defines optional parameters that you can enter after the **no energy-saver schedule** command.

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

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

Configuring AES scheduling to default using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI.
- Disable AES globally.

Procedure steps

Configure AES scheduling by using the following command:

```
default energy-saver schedule
```

Variable definitions

The following table defines optional parameters that you can enter after 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).
weekday	Configures AES scheduling for all weekdays to default (disabled).
weekend	Configures AES scheduling for Saturday and Sunday to default (disabled).
<hh:mm>	Specifies the scheduled AES start time (hour and minutes).

Viewing AES scheduling using ACLI

Use the following procedure to review configured energy saving schedule information.

Prerequisites

Log on to the User EXEC mode in ACLI.

Procedure steps

View AES savings by using the following command:

`show energy-saver schedule`

Job aid: show energy-saver schedule command output

The following figure displays sample output for the **`show energy-saver schedule`** command.

```
ERS-4526FX(config)#show energy-saver schedule
Day        Time  Action
---------- ----- -----------
Monday     08:00 Activate
Wednesday  11:00 Activate
Friday     14:00 Activate
ERS-4526FX(config)#
```

Figure 14: show energy-saver schedule command output

Viewing AES savings using ACLI

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

Prerequisites

Log on to the User EXEC mode in ACLI.

Procedure steps

View AES savings by using the following command:

`show energy-saver savings`

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.

Job aid: show energy-saver savings command output

The following figure displays sample output for the **`show energy-saver savings`** command.

```
4524GT-PWR>show energy-saver savings
Unit# Model        Switch Capacity Saving PoE Saving
----- ------------ ---------------------- -------------------
1     4524GT-PWR   0.0 watts              0.0 watts
-------------------------------------------------------------
TOTAL              0.0 watts              0.0 watts
=============================================================
4524GT-PWR>
```

Figure 15: show energy-saver savings command output

Viewing the global AES configuration using ACLI

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

Prerequisites

Log on to the User EXEC mode in ACLI.

Procedure steps

View the global AES configuration by using the following command:

`show energy-saver`

Job aid: show energy-saver command output

The following figure displays sample output for the **`show energy-saver`** command.

```
ERS-4526FX>show energy-saver
Nortel Energy Saver (NES): Enabled
NES PoE Power Saving Mode: Enabled
NES Efficiency-Mode Mode:  Disabled
Day/Time:                  Thursday 13:33:53
Current NES state:         NES is Inactive
ERS-4526FX>
```

Figure 16: show energy-saver command output

Viewing port-based AES configuration using ACLI

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

Prerequisites

Log on to the User EXEC mode in ACLI.

Procedure steps

View AES savings by using the following command:

```
show energy-saver interface <portlist>
```

Variable definitions

The following table defines optional parameters that you can enter after the **`show energy-saver interface`** command.

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

Job aid: show energy-saver interface command output

The following figure displays sample output for the **`show energy-saver interface`** command using the *<portlist>* variable.

```
ERS-4500(config-if)#sho energy-saver interface 1-6
Port       NES State PoE Savings PoE Priority
---------- --------- ----------- ------------
1          Enabled   N/A         N/A
2          Enabled   N/A         N/A
3          Disabled  N/A         N/A
4          Enabled   N/A         N/A
5          Enabled   N/A         N/A
6          Disabled  N/A         N/A
ERS-4500(config-if)#
```

Figure 17: show energy-saver interface command output

Enabling the Web server for EDM

You must enable the Web server before you can start Enterprise Device Manager. For information about enabling the Web server using ACLI, see *Avaya Ethernet Routing Switch 4500 Series* (NN47205-102.)

Chapter 7: System configuration using Enterprise Device Manager

This chapter provides procedures you can use to configure the switch or stack with Enterprise Device Manager (EDM).

Configuring Quick Start using EDM

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

Procedure steps

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, double-click **Quick Start** .
3. In the IP/Community/Vlan work area, type a switch or stack IP address in the **In-Band Stack IP Address** dialog box.
4. In the **In-Band Stack Subnet Mask** dialog box, type a subnet mask.
5. In the **Default Gateway** dialog box, type an IP address.
6. In the **Read-Only Community String** box, type a character string.
7. In the **Re-enter to verify** dialog box immediately following the Read-Only Community String box, retype the character string from Step 6.
8. In the **Read-Write Community String** dialog box, type a character string.
9. In the **Re-enter to verify** dialog box immediately following the Read-Write Community String: box, retype the character string from Step 8.
10. In the **Quick Start VLAN** dialog box, type a VLAN ID ranging from 1 to 4094.
11. Click **Apply** .

Configuring remote access using EDM

Use this procedure to configure remote access for a switch.

Procedure steps

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

Variable definitions

Use the data in this table to configure remote access for a switch.

Variable	Value
Telnet Remote Access Setting	Specifies the remote access settings for telnet sessions. • Access—allows or disallows telnet access to the switch • Use List—enables (Yes) or disables (No) the use of listed remote Telnet information.
SNMP Remote Access Setting	Specifies SNMP remote access settings.

Variable	Value
	• Access—allows or disallows SNMP access to the switch • Use List—enables (Yes) or disables (No) the use of listed remote SNMP information.
Web Page Remote Access Setting	Specifies web page remote access settings. Use List—enables (Yes) or disables (No) the use of listed remote web page information.
SSH Remote Access Setting	Specifies SSH remote access settings. • Access—allows or disallows SSH access to the switch • Use List—enables (Yes) or disables (No) the use of listed remote SSH information.

Configuring the IPv4 remote access list using EDM

Use this procedure to configure a list of IPv4 source addresses for which to permit remote access to a switch.

Procedure steps

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, double-click **Remote Access** .
3. In the work area, click the **Allowed List(IPv4)** tab.
4. To select a source to edit, click the source row.
5. In the source row, double-click the cell in the **Allowed Source IP Address** column.
6. In the dialog box, type a value.
7. In the source row, double-click the cell in the **Allowed Source Mask** column.
8. In the dialog box, type a value.
9. Click **Apply** .

Variable definitions

Use the data in this table to configure to configure a list of IPv4 source addresses for which to permit access to the switch.

Variable	Value
Allowed Source IP Address	Specifies the source IPv4 address to permit remote access to the switch.
Allowed Source Mask	Specifies subnet mask associated with the source IPv4 address to permit remote access to the switch.

Configuring the IPv6 remote access list using EDM

Use this procedure to configure a list of IPv6 source addresses for which to permit remote access to a switch.

Procedure steps

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, double-click **Remote Access** .
3. In the work area, click the **Allowed List(IPv6)** tab.
4. To select a source to edit, click the source row.
5. In the source row, double-click the cell in the **Allowed Source IPv6 Address** column.
6. In the dialog box, type a value.
7. In the source row, double-click the cell in the **Allowed Prefix Length** column.
8. In the dialog box, type a value.
9. Click **Apply** .

Variable definitions

Use the data in this table to configure to configure a list of IPv6 source addresses for which to permit access to the switch .

Variable	Value
Allowed Source IPv6 Address	Specifies the source IPv6 address to permit remote access to the switch.
Allowed Prefix Length	Specifies prefix length for the source IPv6 address to permit remote access to the switch. Values range from 0 to 128.

Viewing switch unit information using EDM

Use this procedure to display switch specific information.

Procedure steps

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

Variable definitions

Use the data in this table to help you understand the switch unit display.

Variable	Value
Type	Indicates the type number.
Descr	Indicates the type of switch.
Ver	Indicates the version number of the switch.
SerNum	Indicates the number of the switch.
BaseNumPorts	Indicates the base number of ports.
TotalNumPorts	Indicates the total number of ports.

Switch unit PoE management using EDM

Use the information in this section to display and manage power over Ethernet (PoE) for one or more switches in a stack.

Managing PoE for a switch unit using EDM

Use this procedure to display and manage PoE for a single switch unit.

Procedure steps

1. From the Device Physical View, click a switch unit with PoE ports.
2. From the navigation tree, choose Edit.
3. In the Edit tree, double-click **Unit**.
4. In the work area, click the **PoE** tab.
5. In the **UsageThreshold%**, type a value.
6. 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 **PowerDeviceDetectType** section, click a radio button.
8. Click **Apply** .

Variable definitions

Use the data in the following table to display and manage PoE for a switch unit.

Variable	Value
Power(watts)	Displays the total power (in watts) available to the switch.
OperStatus	Displays the power state of the switch: • on • off • faulty
Consumption Power(watts)	Displays the power (in watts) being used by the switch.
UsageThreshold%	Lets you set a percentage of the total PoE power usage at which the switch sends a warning trap message. If the PoE power usage exceeds the threshold and SNMP traps are appropriately configured, the switch sends the

Variable	Value
	pethMainPowerUsageOnNotification trap. If the power consumption exceeds and then falls below the threshold, the switch sends the **pethMainPowerUsageOffNotification** trap. **Important:** You must enable the traps (NotificationControlEnable) to receive a power usage trap.
Notification ControlEnable	Lets you enable or disable sending traps if the switch power usage exceeds the percentage set in the UsageThreshold field.
PowerDevice DetectType	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 **Important:** The default setting is 802.3af. Ensure that this setting matches the setting for the detection type used by the powered devices on this switch.
PowerPresent	Specifies the currently used power source. Available power sources are AC and DC. • A value of **acOnly** indicates that the only power supply is AC. • A value of **dcOnly** indicates that the only power supply is DC. • A value of **acDc** indicates that there are two power supplies; both AC and DC are supplying power

Viewing PoE for multiple switch units using EDM

Use this procedure to display the PoE configuration for one or more switches in a stack.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **PoE**.
3. In the work area, click the **Globals - PoE Units** tab.

Variable definitions

Use the data in the following table to help you understand the global PoE display.

Variable	Value
Power(watts)	Indicates the total power (in watts) available to the switch.
OperStatus	Indicates the power state of the switch: • on • off • faulty This is a read-only cell.
Consumption Power(watts)	Indicates the power (in watts) being used by the switch. This is a read-only cell.
UsageThreshold%	Indicates the 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.
Notification ControlEnable	Indicates whether the sending of traps if the switch power usage exceeds the configured threshold percentage is enabled (true) or disabled (false).
PowerDevice DetectType	Indicates the power detection type that the switch uses to detect a request for power from a device connected to all ports on the switch. Values include: • 802.3af • 802.3af and legacy
PowerPresent	Indicates the currently used power source. Available power sources are AC and DC. • acOnly—indicates that the only power supply is AC • dcOnly—indicates that the only power supply is DC • acDc—indicates that there are two power supplies; both AC and DC are supplying power This is a read-only cell.

Configuring PoE for multiple switch units using EDM

Use this procedure to configure PoE for one or more switches in a stack.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **PoE**.
3. In the work area, click the **Globals - PoE Units** tab.
4. To select a switch to edit, click the Unit.
5. In the Unit row, double-click the cell in the **UsageThreshold%** column.
6. Type a value.
7. In the Unit row, double-click the cell in the **NotificationControlEnable** column.
8. Select a value from the list—**true** to enable the sending of traps if the switch power usage exceeds the configured threshold percentage, or **false** to disable the sending of traps if the switch power usage exceeds the configured threshold percentage .
9. In the Unit row, double-click the cell in the **PowerDeviceDetectType** column.
10. Select a value from the list.
11. To manage PoE for additional switch units in a stack, repeat steps **4** through **10**.
12. Click **Apply** .

Variable definitions

Use the data in the following table to configure PoE for one or more switches in a stack.

Variable	Value
Power(watts)	Indicates the total power (in watts) available to the switch. This is a read-only cell.
OperStatus	Indicates the power state of the switch: • on • off • faulty This is a read-only cell.
Consumption Power(watts)	Indicates the power (in watts) being used by the switch. This is a read-only cell.
UsageThreshold%	Specifies the percentage of the total power usage of the switch above which the system sends a trap.

Variable	Value
	Important: You must enable the traps (NotificationControlEnable) to receive a power usage trap.
Notification ControlEnable	Enables (true) or disables (false) the sending of traps if the switch power usage exceeds the configured threshold percentage.
PowerDevice DetectType	Specifies the power detection type that the switch uses to detect a request for power from a device connected to all ports on the switch. Values include: • 802.3af • 802.3af and legacy **Important:** The default setting is 802.3af. Ensure that this setting matches the setting for the detection type used by the powered devices on this switch.
PowerPresent	Indicates the currently used power source. Available power sources are AC and DC. • acOnly—indicates that the only power supply is AC • dcOnly—indicates that the only power supply is DC • acDc—indicates that there are two power supplies; both AC and DC are supplying power This is a read-only cell.

Configuring system parameters using EDM

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

Procedure steps

1. From the Configuration navigation tree, click the **Edit** arrowhead to open the Edit navigation tree.
2. Double-click **Chassis** .
3. In the Chassis tree, double-click **Chassis**.
4. In the work area, click the **System** tab.
5. In the **sysContact** field, type system contact information.

6. In the **sysName** field, type a system name.
7. In the **sysLocation** field, type a system location.
8. To enable authentication traps, select the **Authentication Traps** check box.

   OR

   To disable authentication traps, clear the **Authentication Traps** checkbox.
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. In the **BootMode** section, click a radio button.
13. Click **Apply** .

Variable definitions

Use the data in this table to view and modify the system level configuration.

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

Variable	Value
	• running—the switch remains in the running mode • reboot—starts the reboot sequence
AutoPvid	When enabled, a VLAN ID can be automatically assigned to any port.
StackInsertionUnitNumber	Specifies the unit number to assign to the next unit added to the stack. Values range from 0–8. You cannot set the value to the unit number of an existing stack member. When a new unit joins the stack, and the value of this object is used as its unit number, the value reverts to 0. If the value of this object is 0, it is not used to determine the unit number of new units.
NextBootMgmtProtocol	Indicates the transport protocols to use after the next switch restart. This is a read-only item.
CurrentMgmtProtocol	Indicates the current transport protocols that the switch supports. This is a read-only item.
BootMode	Specifies whether to use the BootP or DHCP server to assign an IPv4 address for the management VLAN at the next switch reboot. Values include: • other—read only • bootpDisabled—use configured server IP address • bootpAlways—always use the BootP server • bootpWhenNeeded—use the BootP server when needed • bootpOrLastAddress—use the BootP server last used • dhcp—always use the DHCP server • dhcpWhenNeeded—use the DHCP server when needed • dhcpOrLastAddress—use the DHCP server last used

Variable	Value
ImageLoadMode	Indicates the source from which to load the agent image at the next boot. This is a read-only item.
CurrentImageVersion	Indicates the version number of the agent image that is currently used on the switch. This is a read-only item.
LocalStorageImage Version	Indicates the version number of the agent image that is stored in flash memory on the switch. This is a read-only item.
NextBootDefaultGateway	Indicates the IP address of the default gateway for the agent to use after the next time you boot the switch. This is a read-only item.
CurrentDefaultGateway	Indicates the address of the default gateway that is currently in use. This is a read-only item.
NextBootLoadProtocol	Indicates the transport protocol that the agent uses to load the configuration information and the image at the next boot. This is a read-only item.
LastLoadProtocol	Indicates the transport protocol last used to load the image and configuration information about the switch. This is a read-only item.

Configuring asset ID using EDM

Use the following procedure to configure the asset ID of a switch or stack.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. On the work area, click the **Asset ID** tab.
5. In the table, double-click the cell under the **Asset ID** column heading.

6. Type the desired value in the **Asset ID** field.
7. On the toolbar, click **Apply**.

Variable definitions

The following table is an example for a stack of 2 units and you can extend this up to 8 units. Use the data in the following table to complete this procedure.

Variable	Value
Stack	Sets the Asset ID of the stack
Unit 1	Sets the Asset ID of unit 1 in the stack
Unit 2	Sets the Asset ID of unit 2 in the stack

Selecting the ACLI banner type using EDM

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

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. On the work area, click the **Banner** tab.
5. In the **BannerControl** section, click a radio button.
6. Click **Apply**.

Variable definitions

Use the information in the following table to select the ACLI banner type.

Variable	Value
BannerControl	Specifies the banner to be displayed as soon as you connect to an Avaya Ethernet Routing Switch 4500 Series device using Telnet. Values include: • static—uses the predefined static banner. • custom—uses the previously set custom banner. • disabled—prevents the display of any banner.

Customizing ACLI banner using EDM

Use this procedure to customize banner that is displayed on the Avaya Command Line (ACLI) Telnet screen.

Prerequisites

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

Procedure steps

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

Variable definitions

Use the data in this table to customize 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.

Configuring AUR using EDM

Use this procedure to configure automatic unit replacement (AUR).

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. In the work area, select the **AUR** tab.
5. To enable automatic unit replacement, select the **AutoUnitReplacementEnabled** check box.

   OR

   To disable automatic unit replacement, clear the **AutoUnitReplacementEnabled** check box.
6. To enable automatic unit replacement save, select the **AutoUnitReplacementSaveEnabled** check box.

   OR

   To disable automatic unit replacement save, clear the **AutoUnitReplacementSaveEnabled** check box.
7. In the AutoUnitReplacementForceSave dialog box, type a value.
8. In the AutoUnitReplacementRestore dialog box, type a value.
9. Click **Apply** .

Variable definitions

Use the data in this table to configure AUR.

Variable	Value
AutoUnitReplacementEnabled	Enables or disables the auto-unit-replacement feature.
AutoUnitReplacementSaveEnabled	Enables or disables the auto-unit-replacement automatic saving of unit images to the base unit.
AutoUnitReplacementForceSave	Forcefully saves the configuration of a particular non base unit configuration to the base unit.
AutoUnitReplacementRestore	Forcefully restores the configuration of a particular unit from the saved configuration on the base unit.

Configuring a switch stack base unit using EDM

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

Procedure steps

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

Variable definitions

Use the information in the following table to help you understand the base unit information display.

Variable	Value
Type	Indicates the switch type.
Descr	Describes the switch hardware, including number of ports and transmission speed.
Ver	Indicates the switch hardware version number.
SerNum	Indicates the switch serial number.
LstChng	Indicates the value of sysUpTime at the time the interface entered its current operational state. If you entered the current state prior to the last reinitialization of the local network management subsystem, the value is zero.
AdminState	Specifies the administrative state of the base unit switch. Values include enable or reset. **Important:** In a stack configuration, the `reset` command 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 of the switch.
TotalNumPorts	Indicates the number of ports of the switch.
IpAddress	Indicates the base unit IP address.
RunningSoftwareVer	Indicates the version of the running software.

Renumbering stack switch units using EDM

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

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis** .
3. In the Chassis tree, double-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.
7. Select a value from the list.
8. Click **Apply** .

   A warning message appears indicating that initiating the renumbering of switch units in a stack results in an automatic reset of the entire stack.

Variable definitions

Use the information in the following table to change the unit numbers of switches in a stack.

Variable	Value
Current Unit Number	Indicates the current switch numbering sequence.
New Unit Number	Specifies the updated switch numbering sequence.

Interface port management using EDM

Use the information in this section to display and manage switch interface port configurations.

Viewing switch interface port information using EDM

Use this procedure to display switch interface port configuration information.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. Double-click **Ports**.
4. In the work area, click the **Interface** tab.

Variable definitions

Use the data in this table to help you understand the interface port display.

Variable	Value
Index	A unique value assigned to each interface.
Name	Specifies a name for the port.
Descr	The description of the selected port.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	The current administrative state of the device, which can be one of the following: • up • down When a managed system is initialized, all interfaces start with AdminStatus in the up state. AdminStatus changes to the down state (or remains in the up state) because either management action or the configuration information available to the managed system.
OperStatus	The current operational state of the interface, which can be one of the following: • up • down • testing If AdminStatus is up then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down then OperStatus should be down. It should remain in the down state if and only if there is a fault that

Variable	Value
	prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
LinkTrap	Specifies whether linkUp/linkDown traps should be generated for this interface.
AutoNegotiate	Indicates whether this port is enabled for autonegotiation or not. **Important:** 10/100BASE-TX ports can not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question.
AdminDuplex	The current administrative duplex mode of the port (half or full).
OperDuplex	The current mode of the port (half duplex or full duplex).
AdminSpeed	Set the port's speed.
OperSpeed	The current operating speed of the port.
AutoNegotiationCapability	Specifies the port speed and duplex capabilities that a switch can support on a port, and that can be advertised by the port using auto-negotiation.
AutoNegotiation Advertisments	Specifies the port speed and duplex abilities to be advertised during link negotiation.
MltId	The MultiLink Trunk to which the port is assigned (if any).
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	Specifies the physical port components that are active for a shared port.

Changing the configuration for specific interface ports using EDM

Use this procedure to modify configuration parameters for one or more interface ports.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. Double-click **Ports**.
4. In the work area, click the **Interface** tab.
5. To select an interface port to edit, click the **Index**.
6. In the port row, double-click the cell in the **Name** column.
7. Type a character string.
8. In the port row, double-click the cell in the **AdminStatus** column.
9. Select a value from the list.
10. In the port row, double-click the cell in the **LinkTrap** column.
11. From the list, enable or disable link traps for the port.
12. In the port row, double-click the cell in the **AutoNegotiate** column.
13. Select a value from the list—**true** to enable autonegotiation for the port, or **false** to disable autonegotiation for the port.
14. In the port row, double-click the cell in the **AdminDuplex** column.
15. Select a value from the list.
16. In the port row, double-click the cell in the **AdminSpeed** column.
17. Select a value from the list.
18. In the port row, double-click the cell in the **AutoNegotiationAdvertisments** column.
19. Select or clear autonegotiation advertisement check boxes.
20. Repeat steps **6** through **20** to change the configuration for additional interface ports.
21. Click **Ok** .
22. Click **Apply** .

Variable definitions

Use the data in this table to modify configuration parameters for one or more interface ports.

Variable	Value
Index	A unique value assigned to each interface. The value ranges between 1 and 512.
Name	Specifies a name for the port.
Descr	The description of the selected port.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	The current administrative state of the device, which can be one of the following: • up • down When a managed system is initialized, all interfaces start with AdminStatus in the up state. AdminStatus changes to the down state (or remains in the up state) because either management action or the configuration information available to the managed system.
OperStatus	The current operational state of the interface, which can be one of the following: • up • down • testing If AdminStatus is up then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
LinkTrap	Specifies whether linkUp/linkDown traps should be generated for this interface.
AutoNegotiate	Indicates whether this port is enabled for autonegotiation or not. **Important:** 10/100BASE-TX ports can not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions.

Variable	Value
	If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question.
AdminDuplex	The current administrative duplex mode of the port (half or full).
OperDuplex	The current mode of the port (half duplex or full duplex).
AdminSpeed	Set the port speed.
OperSpeed	The current operating speed of the port.
AutoNegotiationCapability	Specifies the port speed and duplex capabilities that a switch can support on a port, and that can be advertised by the port using auto-negotiation.
AutoNegotiation Advertisments	Specifies the port speed and duplex abilities to be advertised during link negotiation.
MltId	The MultiLink Trunk to which the port is assigned (if any).
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	Specifies the physical port components that are active for a shared port.

PoE configuration for switch ports using EDM

Use the information in this section to display and modify PoE configurations for switch ports.

Important:
The procedures in this section apply only to a switch with PoE ports.

Viewing PoE information for specific switch ports using EDM

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

Procedure steps

1. From the Device Physical View, select one or more ports.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.

4. Double-click **Ports**.
5. In the work area, click the **PoE** tab.

Variable definitions

Use the data in the following table to display the PoE configuration for specific switch ports.

Variable	Value
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Lets you enable or disable PoE on this port. By default, PoE is enabled.
DetectionStatus	Displays the operational status of the power-device detecting mode on the specified port: • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power • fault—power-specific fault detected on port • test—detecting device in test mode • otherFault **Important:** Avaya recommends against using the test operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
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. The default value is 16W.
Voltage(volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

Configuring PoE for specific switch unit ports using EDM

Use this procedure to modify the PoE configuration for a one or more ports on a specific switch unit.

Procedure steps

1. From the Device Physical View, select one or more ports on a switch unit.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. Double-click **Ports**.
5. In the work area, click the **PoE** tab.
6. In the unit port row, double-click the cell in the **AdminEnable** column.
7. Select a value from the list—**true** to enable PoE for the port, or **false** to disable PoE for the port.
8. In the unit port row, double-click the cell in the **PowerPriority** column.
9. Select a value from the list.
10. In the unit port row, double-click the cell in the **PowerLimit(watts)** column.
11. Type a value.
12. To configure PoE for other selected ports, repeat steps **6** through **11** .
13. Click **Apply** .

Variable definitions

Use the data in the following table to modify PoE for a one or more specific ports.

Variable	Value
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Lets you enable or disable PoE on this port. By default, PoE is enabled.

Variable	Value
DetectionStatus	Displays the operational status of the power-device detecting mode on the specified port: • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power • fault—power-specific fault detected on port • test—detecting device in test mode • otherFault **Important:** Avaya recommends against using the test operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
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. The default value is 16W.
Voltage(volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

Configuring PoE for switch or stack ports using EDM

Use this procedure to modify the PoE configuration for a one or more switch or stack ports.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **PoE**.

3. In the work area, click the **PoE Ports** tab.
4. To select a switch port to edit, click the unit row.
5. In the unit port row, double-click the cell in the **AdminEnable** column.
6. Select a value from the list—**true** to enable PoE for the port, or **false** to disable PoE for the port.
7. In the unit port row, double-click the cell in the **PowerPriority** column.
8. Select a value from the list.
9. In the unit port row, double-click the cell in the **PowerLimit(watts)** column.
10. Type a value.
11. To configure PoE for additional ports, repeat steps **4** through **10** .
12. Click **Apply** .

Variable definitions

Use the data in the following table to configure PoE for a one or more switch or stack ports.

Variable	Value
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Lets you enable or disable PoE on this port. By default, PoE is enabled.
DetectionStatus	Displays the operational status of the power-device detecting mode on the specified port: • disabled—detecting function disabled • searching—detecting function is enabled and the system is searching for a valid powered device on this port • deliveringPower—detection found a valid powered device and the port is delivering power • fault—power-specific fault detected on port • test—detecting device in test mode • otherFault **Important:** Avaya recommends against using the test operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such

Variable	Value
	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. The default value is 16W.
Voltage(volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

Configuring Rate Limiting using EDM

Use the following procedure to configure the Rate Limiting for a single port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. On the work area, click the **Rate Limit** tab.
5. To a rate limit, click a **TrafficType** row.
6. Double-click the cell in the **AllowedRate** column.
7. Select a value from the list.
8. Double-click the cell in the **Enable** column.
9. Select a value from the list—**true** to enable the traffic type, or **false** to disable the traffic type.

Variable definitions

Use the data in this table to configure rate limiting.

Variable	Value
Index	Indicates the unique identifier.
TrafficType	Specifies the two types of traffic that can be set with rate limiting: broadcast and multicast.
AllowedRate	Specifies the rate limiting percentage. The available range is from 0 percent (none) to 10 percent.
Enable	Enables and disables rate limiting on the port for the specified traffic type. Options are true (enabled) or false (disabled).

Managing switch software using EDM

Use this procedure to change the binary configuration running on the switch, upload the configuration file to a TFTP server or a USB storage device, or retrieve a binary configuration file from a TFTP server.

Important:
When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

Procedure steps

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

The software download starts automatically after you click Apply. This process erases the contents of flash memory, and replaces it with the new software image. Do not interrupt the download. Depending on network conditions, this process can take up to 10 minutes. After the download is complete, the switch automatically resets, and the new software image initiates a self-test. During the download, the switch is not operational.

Variable definitions

Use the information in the following table to help you to understand the fields of Config/Image/Diag file tab.

Variable	Value
TftpServerInetAddressType	Specifies the type of TFTP address. • IPv4 • IPv6
TftpServerInetAddress	Specifies the IP address of the TFTP server on which the new software images are stored for download.
BinaryConfigFileName	Specifies the binary configuration file currently associated with the switch. Use this dialog box when you work with configuration files; do not use this dialog box when you download a software image.
BinaryConfigUnitNumber	Specifies the binary configuration unit number. Values range from 0 to 8. The default value is 0.
ImageFileName	Specifies the name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.
FwFileName (Diagnostics)	Specifies the name of the diagnostic file currently associated with the switch. If needed, change this field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	Specifies the unit number of the USB port to be used to upload or download a file. Values range from 0 to 9. • 1 to 8—a USB port in a stack • 9—a USB port in a standalone switch • 0—TFTP server
Action	Represents the actions taken during this file system operation. The available options are as follows: • other—read only • dnldConfig—downloads a configuration to the switch.

Variable	Value
	• upldConfig—uploads a configuration from the switch to a designated location. • dnldConfigFromUsb—downloads a configuration to switch using the front panel USB port. • upldConfigToUsb—uploads a configuration from the switch to the server using the front panel USB port. • dnldImg—downloads a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. • dnldImgIfNewer—downloads a new software image to the switch only if it is newer than the one currently in use. • dnldImgNoReset—downloads a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • dnldImgFromUsb—downloads a new software image to the switch using the front panel USB port. • dnldFw—downloads a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. • dnldFwNoReset—downloads a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset. • dnldFwFromUsb—downloads a new diagnostic software image to the switch from the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image.
Status	Displays the status of the last action that occurred since the switch last booted. Values include: • other—no action occurred since the last boot. • inProgress—the selected operation is in progress. • success—the selected operation succeeded. • fail—the selected operation failed.

ASCII configuration file management using EDM

Use the information in this section to store or retrieve an ASCII configuration file.

ASCII configuration file management prerequisites

Read and understand the detailed information about ASCII configuration files in *Avaya Ethernet Routing Switch 4500 Series Fundamentals* (NN47205-102).

Storing the current ASCII configuration file using EDM

Use the following procedure to store the current ASCII switch configuration file to a TFTP server or USB storage device.

Important:
When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **File System**.
3. In the work area, click the **ASCII Config Script Files** tab.
4. To select a script file, click the script index.
5. In the script row, double-click the cell in the **ScriptBootPriority** column.
6. Type a value.
7. In the script row, double-click the cell in the **ScriptSource** column.
8. Type the IP address of the desired TFTP server and the name under which to store the configuration file in the format— tftp://<ip address>/<filename>.

   If the configuration file is saved to a USB storage device, type the name under which to store the configuration file in the following format—usb://<filename>.

   If the USB is inserted in a stand-alone unit, or if the USB device is inserted in a unit of a stack, type usb://<unit number>/<filename>.

9. Double-click the cell under the **ScriptManual** header, and select **Upload** option to transfer the file to a TFTP server or to a USB mass storage device.
10. On the toolbar, click **Apply**.
11. Check the **ScriptLastStatusChange** field for the file transfer status.

    If the status of the file upload is manualUploadInProgress, wait for up to 2 minutes, and then click **Refresh** to see any new status applied to the upload.

    The file upload is complete when the status displays either manualUploadPassed or manualUploadFailed.
12. Click **Apply** .

Variable definitions

Use the information in the following table to help you to store the current ASCII switch configuration file.

Variable	Value
ScriptIndex	Specifies the unique identifier for ASCII switch configuration file.
ScriptBootPriority	Specifies the boot priority of the ASCII switch configuration file. Value ranges from 0–127.
ScriptSource	Specifies the address where to store the configuration file.
ScriptManual	Specifies the operation that you want to perform—upload, download, or other.
Applications	Specifies the application.
ScriptOperStatus	Specifies the script operation status.
ScriptLastStatusChange	Specifies the time of the last status change as sysUpTime.

Retrieving an ASCII configuration file using EDM

Use the following procedure to retrieve an ASCII configuration file from a TFTP server or from a USB storage device, and apply it to the switch.

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **File System**.
3. On the work area, click the **ASCII Config Script Files** tab.
4. In the table, double-click the cell under the **ScriptSource** heading for the parameter you want to change.
5. Type the IP address of the desired TFTP server and the name under which to store the configuration file in the format— tftp://<ip address>/<filename>.

   If you retrieve the configuration file from a USB storage device, and the USB is inserted in a stand-alone unit, type the name under which to store the configuration file in the following format—usb://<filename>.

   If the USB device is inserted in a unit of a stack, type usb://<unit number>/<filename>.
6. Double-click the cell under the **ScriptManual** header, and select **Download** option to transfer the file from a TFTP server or from a USB mass storage device.
7. On the toolbar, click **Apply**.
8. Check the **ScriptLastStatusChange** field for the file transfer status.

   If the status of the file download is manualDownloadInProgress, wait for up to 2 minutes, and then click **Refresh** to see any new status applied to the upload.

   The file downlaod is complete when the status displays either **manualDownloadPassed** or **manualDownloadFailed**.

Automatically downloading a configuration file using EDM

Use the following procedure to download a configuration file automatically.

Important:

When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

Procedure steps

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **File System**.
3. On the work area, click the **ASCII Config Script Files** tab.
4. In the table, double click the cell under the **ScriptSource** header.
    - If you retrieve the configuration file from a TFTP server, type the IP address of the desired TFTP server and the name under which the configuration file is stored in the following format—`tftp://<ip address>/<filename>`.
    - If you retrieve the configuration file from a USB storage device, and the USB device is inserted in a stand-alone unit, type the name under which the configuration file is stored in the following format—`usb://<filename>`.
    - If you retrieve the configuration file from a USB storage device, and the USB device is inserted in a unit of a stack, type the name under which the configuration file is stored in the following format— `usb://<unit number>/<filename>`.
    - If you retrieve the file from a BOOTP server, type `bootp://`.
5. Double-click the cell under the **ScriptBootPriority** header.
6. Type the priority of the script (between 1 and 127, or 0 for not using the entry at boot time).
7. On the toolbar, click **Apply**.

Managing the license file using EDM

Use this procedure to download, install, or remove a license file for the switch.

Important:
When you use the TFTP address parameter to perform copy or download commands, the system overwrites the TFTP server address

Procedure steps

1. From the navigation tree, double-click **Edit** .
2. In the Edit tree, double-click **File System**.

3. In the work area, select the **License File** tab.
4. In the **TftpServerInetAddressType** section, click a radio button.
5. In the **TftpServerInetAddress** dialog box, type the TFTP server IP address.
6. In the LicenseFileName dialog box, enter the software license filename on the TFTP server.

   Important:
   The LicenseFileName dialog box is case sensitive and you can use a maximum of 64 characters including the file extension. Numerals are allowed in the LicenseFileName dialog box, but special characters like @, -, #, are not allowed.
7. In the **UsbTargetUnit** dialog box, type a value.
8. In the LicenseFileAction section, click the **dnldLicense** radio button.
9. In the **Remove License** section, select a value from the list, to remove one or all licenses.
10. Click **Apply**.

    When the file installation is complete, a warning message appears prompting you to restart the switch to activate the license.

    For information about restarting the switch, see Configuring system parameters using EDM on page 220.

Saving the current configuration using EDM

The configuration currently in use on a switch is regularly saved to the flash memory automatically. However, you can manually initiate this process using the **Save Configuration** tab.

Use the following procedure to save the current configuration manually.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **File System**.
3. On the work area, click the **Save Configuration** tab.
4. Select the **AutosaveToNvramEnabled** check box to enable automatically saving the configuration to the flash memory.

OR

Clear the **AutosaveToNvramEnabled** check box to disable automatically saving the configuration to the flash memory.

5. Choose **copyConfigToNvram** in the **Action** field.
6. On the toolbar, click **Apply**.
7. Click **Refresh**.

Variable definitions

Use the information in the following table to save the current configuration.

Variable	Value
AutosaveToNvramEnabled	If selected, automatically saves the configuration to the flash memory.
Action	Indicates the action that you want to perform. Available options are: • other • copyConfigToNvram
Status	Indicates the current status.

Viewing the agent and image software load status using EDM

Use the following procedure to display the currently loaded and operational software status for agent and image loads for an individual switch or a stack.

Procedure steps

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

Variable definitions

Use the data in this table to help you understand the currently loaded and operational software status display.

Variable	Value
Unit 1 Software Image version	Indicates the loaded agent software image for the switch or stack.
Unit 1 Software Image in flash	Indicates the operational agent software image for the switch or stack.
Unit 1 Diag Image version	Indicates the loaded diagnostic software image for the switch or stack.
Unit 1 Diag Image in flash	Indicates the operational diagnostic software image for the switch or stack.

Important:
When the currently loaded and operational software status is displayed for a stack, the unit number is replaced by the word **All**.

Configuring IPv6 global properties using EDM

Use the following procedure to configure IPv6 global properties.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Globals** tab.
4. Configure the IPv6 globally.
5. On the toolbar, click **Apply** to save the changes.
6. Click **Refresh** to display updated information.

Variable definitions

Use the data in this table to help you configure IPv6 globally.

Variable	Value
AdminEnabled	Enables or disables administration function.
OperEnabled	Enables or disables the operation.
Forwarding	Indicates whether this acts as a router or not.
DefaultHopLimit	Indicates the Hop Limit. Default number of hops— 30
IcmpNetUnreach	Enables or disables the ICMP net unreach feature.
IcmpRedirectMsg	Enables or disables ICMP redirect message feature.
IcmpErrorInterval	Indicates the time to wait before sending an ICMP error message. A value of 0 means the system does not send an ICMP error message. Range is 0–2147483647 ms.
IcmpErrorQuota	Indicates the number of ICMP error messages that can be sent out during ICMP error interval. Default value: 1
MulticastAdminStatus	Indicates the admin status for multicast for this interface.

IPv6 interface management using EDM

Use the information in this section to view, create, or delete IPv6 interfaces.

Viewing IPv6 interfaces using EDM

Use the following procedure to view an IPv6 interface ID to a VLAN to learn the ID.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Interfaces** tab.

Variable definitions

Use the data in this table to help you understand the Interfaces tab.

Variable	Value
IfIndex	Identifies a physical interface or a logical interface (VLAN). For a VLAN, it is the Ifindex of the VLAN.
Identifier	Specifies the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
IdentifierLength	Specifies the length of the interface identifier in bits.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.
VlanId	Identifies the Virtual LAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	Specifies Unicast, the only supported type.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1280.
PhysAddress	Specifies the media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true).
OperStatus	Specifies whether the operation status of the interface is up or down.
ReachableTime	Specifies the time (3600000 ms) that a neighbor is considered reachable after receiving a reachability confirmation.
RetransmitTime	Specifies the RetransmitTime, which is the time (3600000 ms) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.
MulticastAdminStatus	Specifies the multicast status as either True or False.

Creating an IPv6 interface using EDM

Use the following procedure to create an IPv6 interface.

Prerequisites

- Ensure that VLAN is configured before you assign an interface identifier, or an IPv6 address to the VLAN.
- The Avaya Ethernet Routing Switch 4500 supports port-based and protocol-based VLANs. For more information about configuring VLANs, see *Avaya Ethernet Routing Switch 4500 Configuration — VLANs, Spanning Tree and Multi-Link Trunking,* (NN47205-501).

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Interfaces** tab.
4. On the toolbar, click **Insert**.
5. Configure the IPv6 interface.
6. Click **Insert**.
7. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to create an IPv6 interface.

Variable	Value
IfIndex	Identifies a physical interface or a logical interface (VLAN). For a VLAN, it is the Ifindex of the VLAN.
Identifier	Specifies the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. Value: 1280–9600

Variable	Value
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false).
ReachableTime	Specifies the time (in milliseconds) that a neighbor is considered reachable after receiving a reachability confirmation. Value: 0–36000000 ms
RetransmitTime	Specifies the RetransmitTime, which is the time (in milliseconds) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Value: 0–36000000 ms

Deleting an IPv6 interface using EDM

Use the following procedure to delete an IPv6 interface.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Interfaces** tab.
4. To select an interface to delete, click the **IfIndex**.
5. Click **Delete** .

Graphing IPv6 Interface Statistics using EDM

Use the following procedure to display and graph IPv6 interface statistics for a switch or stack.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.

3. On the work area, click the **Interfaces** tab.
4. In the table, select the **IfIndex** you want to view.
5. On the toolbar, click **Graph**.

Variable definitions

The following table defines the variables for the Static Routes window

Variable	Value
InReceives	Indicates the total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	Indicates the number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
InNoRoutes	Indicates the number of input IP datagrams discarded because no route is found to transmit them to their destination.
InAddrErrors	Indicates the number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
InUnknownProtos	Indicates the number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InTruncatedPkts	Indicates the number of input IP datagrams discarded because the datagram frame did not carry enough data.
InDiscards	Indicates the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack

Variable	Value
	of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	Indicates the total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutForwDatagrams	Indicates the number of datagrams for which this entity was not their final IP destination and for which it was successful in finding a path to their final destination. In entities that do not act as IP routers, this counter will include only those datagrams that were Source-Routed through this entity, and the Source-Route processing was successful.
OutRequests	Indicates the total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	Indicates the number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). **Note:** This counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutFragOKs	Indicates the number of IP datagrams that are successfully fragmented.
OutFragFails	Indicates the number of IP datagrams that are discarded because they needed to be fragmented but are not. This includes IPv4 packets that have the DF bit set and IPv6 packets that are being forwarded and exceed the outgoing link MTU.
OutFragCreates	Indicates the number of output datagram fragments that are generated because of IP fragmentation.
ReasmReqds	Indicates the number of IP fragments received which needed to be reassembled at this entity.

Variable	Value
ReasmOKs	Indicates the number of IP datagrams successfully reassembled.
ReasmFails	Indicates the number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
InMcastPkts	Indicates the number of IP multicast datagrams received.
OutMcastPkts	Indicates the number of IP multicast datagrams transmitted.

Important:

You can also change the **Poll Interval** by selecting and clicking on a value from the drop down list. The default value for the **Poll Interval** is 10ms.

Configuring an IPv6 address using EDM

Use this procedure to configure an IPv6 address for a switch or stack.

Procedure steps

1. From the navigation tree, double-click **IPv6** .
2. In the IPv6 tree, double-click **IPv6**.
3. In the work area, click the **Addresses** tab.
4. Click **Insert**.
5. Accept the default **IfIndex** value.

   OR

   Click **Vlan** to select a value from the list.
6. In the **Addr** box, type an IPv6 address.
7. In the **AddrLen** box, type the IPv6 prefix length.
8. In the **Type** section, click a radio button.

9. Click **Insert**.
10. Click **Apply** .

Variable definitions

Use the data in the following table to help you configure an IPv6 address for a switch or stack.

Variable	Value
IfIndex	This is the Ifindex of the VLAN.
Addr	Indicates the interface IPv6 address.
AddrLen	Indicates the interface IPv6 prefix length.
Type	Specifies the interface address type. Values include: • unicast • anycast
Origin	Indicates the origin of the interface address. Values include: • other • manual • dhcp • linklayer • random
Status	Indicates the status of the interface address. Values include: • preferred • deprecated • invalid • inaccessible • unknown • tentative • duplicate
Created	Indicates the value of the system up time when this address was created. A value of 0 indicates that this address was created before the last network management subsystem initialization.
LastChanged	Indicates the value of the system up time when this address was last updated. A value of 0 indicates that this address was updated before the last network management subsystem initialization.

Configuring IPv6 static routes using EDM

Use the following procedure to configure IPv6 static routes for a switch or stack.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Static Routes** tab.
4. On the toolbar, click **Insert**.

   The Insert Static Routes dialog box appears.
5. Configure the parameter as required.
6. Click **Insert** to save the changes.

Variable definitions

The following table defines the variables for the Static Routes window.

Variable	Value
Dest	Specifies the destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries depends on the table-access mechanisms defined by the network management protocol in use.
PrefixLength	Indicates the number of leading one bits which form the mask to be logical-ANDed with the destination address before being compared to the value in the rcIpv6StaticRouteDestAddr field.
NextHop	Specifies the IP address of the next hop of this route. (In the case of a route bound to an interface which is realized through a broadcast media, the value of this field is the agent's IP address on that interface).

Variable	Value
IfIndex	Specifies the index value which uniquely identifies the local interface through which the next hop of this route is reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
Status	Used to create or delete entries.

IPv6 neighbor cache management using EDM

Use the information in this section to view and configure the IPv6 neighbor cache.

Viewing the IPv6 neighbor cache using EDM

View the neighbor cache to discover information about neighbors in your network. Neighbor cache in IPv6 is similar to the IPv4 Address Resolution Protocol (ARP) table. The neighbor cache is a set of entries for individual neighbors to which traffic was sent recently. You make entries on the neighbor on-link unicast IP address, including information such as the link-layer address. A neighbor cache entry contains information used by the Neighbor Unreachability Detection algorithm, including the reachability state, the number of unanswered probes, and the time the next Neighbor Unreachability Detection event is scheduled.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Neighbors** tab.

Variable definitions

Use the data in this table to help you view the Neighbors tab.

Variable	Value
IfIndex	Specifies a unique Identifier of a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN.

Variable	Value
NetAddress	Indicates the IP address corresponding to the media-dependent physical address.
PhysAddress	Indicates the media-dependent physical address. The range is 0–65535. For Ethernet, this is a MAC address.
Interface	Indicates either a physical port ID or the Multi-Link Trunking port ID. This entry is associated either with a port or with the Multi-Link Trunking in a VLAN.
LastUpdated	Specifies the value of sysUpTime at the time this entry was last updated. If this entry was updated prior to the last reinitialization of the local network management subsystem, this object contains a zero value.
Type	Specifies the types of mapping. • Dynamic type—indicates that the IP address to the physical address mapping is dynamically resolved using, for example, IPv4 ARP or the IPv6 Neighbor Discovery Protocol. • Static type—indicates that the mapping is statically configured. • Local type—indicates that the mapping is provided for the interface address. The default is static.
State	Specifies the Neighbor Unreachability Detection state for the interface when the address mapping in this entry is used. If Neighbor Unreachability Detection is not in use (for example, for IPv4), this object is always unknown. Options include the following: • reachable—confirmed reachability • stale—unconfirmed reachability • delay—waiting for reachability confirmation before entering the probe state • probe—actively probing • invalid—an invalidated mapping

Variable	Value
	• unknown—state cannot be determined • incomplete—address resolution is being performed

Configuring the IPv6 neighbor cache using EDM

Use the following procedure to configure the IPv6 neighbor cache.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**
3. On the work area, click the **Neighbors** tab.
4. On the toolbar, click **Insert**.
5. Configure the parameters as required.
6. Click **Insert**.
7. Click **Apply**.

Variable definitions

The following table lists the fields in the Insert Neighbors dialog box.

Variable	Value
IfIndex	Indicates a unique identifier to a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN.
NetAddress	Indicates the IP address corresponding to the media-dependent physical address.
PhysAddress	Indicates the media-dependent physical address. The range is 0–65535. For Ethernet, this is a MAC address.
Interface	Indicates either a physical port ID or the Multi-Link Trunking port ID. This entry is associated either with a port or with the Multi-Link Trunking in a VLAN.

Deleting the IPv6 neighbor cache using EDM

Use this procedure to delete the IPv6 neighbor cache.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Neighbors** tab.
4. To select an cache to delete, click the **IfIndex**.
5. Click **Delete** .

Graphing IPv6 interface ICMP statistics using EDM

Use the following procedure to display and graph the IPv6 ICMP statistics.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **ICMP Stats** tab.
4. Click **Clear Counters** to reset the statistics.
5. Configure the **Poll interval** as required.
6. Highlight a data column to graph.
7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

The following table lists the fields in the ICMP Stats tab.

Variable	Value
InMsgs	Indicates the number of ICMP messages received.

Variable	Value
InErrors	Indicates the number of ICMP error messages received.
OutMsgs	Indicates the number of ICMP messages sent.
OutErrors	Indicates the number of ICMP error messages sent.
Poll Interval	Sets polling interval. Value: 2–60 s.

Viewing ICMP message statistics using EDM

Use the following procedure to display the IPv6 interface ICMP message statistics.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **ICMP Msg Stats** tab.
4. On the toolbar, click **Refresh** to update the ICMP message statistics.

Variable definitions

Use the data in the following table to display ICMP message statistics.

Variable	Value
Type	Indicates the type of packet received or sent.
InPkts	Indicates the number of packets received.
OutPkts	Indicates the number of packets sent.

Displaying IPv6 TCP global properties using EDM

Use the following procedure to display IPv6 TCP global properties.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **TCP/UDP**.
3. On the work area, click the **TCP Globals** tab.
4. Click **Refresh** to update the information.

Variable definitions

Use the data in the following table to display IPv6 TCP global properties.

Variable	Value
RtoAlgorithm	Indicates the algorithm identifier.
RtoMin	Indicates the minimum value in milliseconds.
RtoMax	Indicates the maximum value in milliseconds.
MaxConn	Indicates the maximum number of connections.

Displaying IPv6 TCP connections using EDM

Use the following procedure to display IPv6 TCP connections.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **TCP/UDP**.
3. On the work area, click the **TCP Connections** tab.
4. Click **Refresh** to update the information.

Variable definitions

Use the data in the following table to display IPv6 TCP connections.

Variable	Value
LocalAddress	Indicates the local address.
LocalAddressType	Indicates the type of the local address.
LocalPort	Indicates the local port.
RemAddressType	Indicates the type of the remote address.
RemAddress	Indicates the remote address.
RemPort	Indicates the remote port.
State	Enables or disables the state.

Displaying IPv6 TCP listeners using EDM

Use the following procedure to display IPv6 TCP listeners.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **TCP/UDP**.
3. On the work area, click the **TCP Listeners** tab.
4. Click **Refresh** to update the information.

Variable definitions

Use the data in the following table to display IPv6 TCP listeners.

Variable	Value
LocalAddressType	Indicates the local IP address type. Values include IPv4 or IPv6.
LocalAddress	Indicates the local IPv4 or IPv6 address.

Variable	Value
Local Port	Indicates the local port.

Displaying IPv6 UDP endpoints using EDM

Use the following procedure to display IPv6 UDP endpoints.

Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **TCP/UDP**.
3. On the work area, click the **UDP Endpoints** tab.
4. Click **Refresh** to update the information.

Variable definitions

Use the data in the following table to display IPv6 UDP endpoints.

Variable	Value
LocalAddressType	Indicates the local address.
LocalAddress	Indicates the local address port.
Local Port	Indicates the local port.
RemoteAddressType	Indicates the remote address type.
RemoteAddress	Indicates the remote address.
RemotePort	Indicates the remote port.
Instance	Indicates the instance.
Process	Indicates the process.

Viewing SFP GBIC ports using EDM

Use the following procedure to view the SFP GBIC ports.

Prerequisites

Ensure that the SFP GBIC port is active.

Procedure steps

1. From the **Device Physical View**, click a unit.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double click **Chassis**.
4. In the Chassis tree, double-click **Ports**.

Initiating a cable diagnostic test using EDM

Use this procedure to initiate and display results for a cable diagnostic test on a specific switch port, using the Time Domain Reflectometer (TDR).

Procedure steps

1. From the **Device Physical View** right-click a port.
2. Click **Edit**.
3. In the work area, click the **TDR** tab.
4. Select the **StartTest** check box.
5. Click **Apply**.

Variable definitions

Use the data in this table to initiate a cable diagnostic test and help you understand the TDR display.

Variable	Value
StartTest	When selected, enables the cable diagnostic test.

Variable	Value
TestDone	Indicates whether the TDR test is complete (true) or not (false).
CableStatus	Indicates the status of the cable as a summation of the status of the cable conductor pairs. • 1—Fail: the cable is experiencing any combination of open and shorted pairs • 2—Normal: the cable is operating normally with no fault found
Pair1Status	Indicates the status of the first pair in the cable. Values include: • 1—pairFail • 2—pairNormal • 3—pairOpen • 4—pairShorted • 5—pairNotApplicable • 6—pairNotTested • 7—pairForce • 8—pinShort **Important:** If a 10MB or 100MB link is established without autonegotiation, Pair 1 returns Forced mode. The pair length is meaningless in this case.
Pair1Length	Indicates the length of the first pair in the cable, in meters, measured by the TDR.
Pair2Status	Indicates the status of the second pair in the cable. Values include: • 1—pairFail • 2—pairNormal • 3—pairOpen • 4—pairShorted • 5—pairNotApplicable • 6—pairNotTested • 7—pairForce • 8—pinShort

Variable	Value
Pair2Length	Indicates the length of the second pair in the cable, in meters, measured by the TDR.
Pair3Status	Indicates the status of the third pair in the cable. Values include: • 1—pairFail • 2—pairNormal • 3—pairOpen • 4—pairShorted • 5—pairNotApplicable • 6—pairNotTested • 7—pairForce • 8—pinShort
Pair3Length	Indicates the length of the third pair in the cable, in meters, measured by the TDR.
Pair4Status	Indicates the status of the fourth pair in the cable. Values include: • 1—pairFail • 2—pairNormal • 3—pairOpen • 4—pairShorted • 5—pairNotApplicable • 6—pairNotTested • 7—pairForce • 8—pinShort
Pair4Length	Indicates the length of the third pair in the cable, in meters, measured by the TDR.
CableLength	Indicates the length of cable, in meters, based on average electrical length of 4 pairs. This measurement can be performed whether or not network traffic is present on the cable.
Pair1Polarity	Indicates the polarity of the first pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity. Values include:

Variable	Value
	• 1—inversed • 2—normal • 3—invalid
Pair1Swap	Indicates the status of the pin assignments for the first pair in the cable. Values include: • 1—normal • 2—swapped • 3—invalid • 4—error
Pair1Skew	Indicates the differential length, in meters, of the first pair in the cable. The skew measurement can be performed only when the cable gigabit link is up, regardless of traffic activity. A value of –1 means an error occurred with the length measurement.
Pair2Polarity	Indicates the polarity of the second pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity. Values include: • 1—inversed • 2—normal • 3—invalid
Pair2Swap	Indicates the status of the pin assignments for the second pair in the cable. Values include: • 1—normal • 2—swapped • 3—invalid • 4—error
Pair2Skew	Indicates the differential length, in meters, of the second pair in the cable. The skew measurement can be performed only when the cable gigabit link is up, regardless of traffic activity. A value of –1 means an error occurred with the length measurement.
Pair3Polarity	Indicates the polarity of the third pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity. Values include:

Variable	Value
	• 1—inversed • 2—normal • 3—invalid
Pair3Swap	Indicates the status of the pin assignments for the third pair in the cable. Values include: • 1—normal • 2—swapped • 3—invalid • 4—error
Pair3Skew	Indicates the differential length, in meters, of the third pair in the cable. The skew measurement can be performed only when the cable gigabit link is up, regardless of traffic activity. A value of –1 means an error occurred with the length measurement.
Pair4Polarity	Indicates the polarity of the fourth pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity. Values include: • 1—inversed • 2—normal • 3—invalid
Pair4Swap	Indicates the status of the pin assignments for the fourth pair in the cable. Values include: • 1—normal • 2—swapped • 3—invalid • 4—error
Pair4Skew	Indicates the differential length, in meters, of the fourth pair in the cable. The skew measurement can be performed only when the cable gigabit link is up, regardless of traffic activity. A value of –1 means an error occurred with the length measurement.

Viewing basic system bridge information using EDM

Use this procedure to display system bridge information, including the MAC address, type, and number of ports participating in the bridge.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **Base** tab.

Variable definitions

Variable	Value
BridgeAddress	Indicates the MAC address of the bridge when it is uniquely referred to. This address must be the smallest MAC address of all ports that belong to the bridge. However, it must be unique. When concatenated with dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol.
NumPorts	Indicates the number of ports controlled by the bridging entity.
Type	Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this fact is indicated by entries in the port table for the given type.

Viewing transparent bridge information using EDM

Use this procedure to display information about learned forwarding entry discards and to configure the aging time.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **Transparent** tab.
4. In the **AgingTime** dialog box, type a value.
5. On the toolbar, click **Apply**.

Variable definitions

Variable	Value
LearnedEntryDiscards	Indicates the number of Forwarding Database entries learned discarded due to insufficient space in the Forwarding Database. If this counter increases, it indicates that the Forwarding Database is becoming full regularly. This condition affects the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has occurred but is not persistent.
AgingTime	Indicates the time-out period in seconds for removing old dynamically learned forwarding information. **Important:** The 802.1D-1990 specification recommends a default of 300 seconds.

Viewing forwarding bridge information using EDM

Use this procedure to display information about bridge forwarding status.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **Forwarding** tab.

4. To select specific bridge port status information display criteria, click **Filter**.
5. Select filtering criteria.
6. Click **Filter** .

Variable definitions

Use the data in the following table to help you understand the bridge port status display.

Variable	Value
Id	Specifies the VLAN identifier.
Address	Indicates the unicast MAC address for which the bridge has forwarding or filtering information.
Port	Indicates the port number. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress A value of 0 indicates that the port number has not been learned, so the bridge does have the forwarding or filtering information for this address (in the dot1dStaticTable). You must assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned.
Status	Indicates the values for this field include: • invalid: Entry is no longer valid, but has not been removed from the table. • learned: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used. • self: Value of the corresponding instance of dot1dTpFdbAddress represents an address of the bridge. The corresponding instance of dot1dTpFdbPort indicates that a specific port on the bridge has this address. • mgmt(5): Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress. • other: None of the preceding. This includes instances where another MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is used to determine if frames addressed to the value of dot1dTpFdbAddress are being forwarded.

Graphing port bridge statistics using EDM

Use the following procedure to graph port bridge statistical information.

Procedure steps

1. From the Device Physical View, click a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port** .
4. In the work area, click the **Bridge** tab.
5. On the toolbar, select a value from the **Poll Interval** list.
6. To reset the statistics counters, click **Clear Counters**.
7. To select bridge statistical information to graph, click a data row under a column heading.
8. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**column.

Variable definitions

Use the data in the following table to help you understand port bridge statistics.

Variable	Value
DelayExceededDiscards	Number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges.
MtuExceededDiscards	Number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges.
InFrames	The number of frames that have been received by this port from its segment.
OutFrames	The number of frames that have been received by this port from its segment.
InDiscards	Count of valid frames received which were discarded (filtered) by the Forwarding Process.

Configuring SNTP using EDM

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

Procedure steps

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

Variable definitions

Use the data in this table to configure SNTP.

Variable	Value
PrimaryServerInetAddress Type	Specifies the primary SNTP server IP address type. Values include ipv4 and ipv6.
PrimaryServerInetAddress	Specifies the IP address of the primary SNTP server.
SecondaryServerInetAddress Type	Specifies the secondary SNTP server IP address type. Values include ipv4 and ipv6.
SecondaryServerInetAddress	Specifies the IP address of the secondary SNTP server.
State	Specifies if the switch uses SNTP to synchronize the switch clock to the Coordinated Universal Time (UTC). • disabled—the device cannot synchronize its clock using SNTP • enabled (unicast)—the device synchronizes to UTC shortly after start time when network access becomes available, and periodically thereafter

Variable	Value
SynchInterval	Specifies the frequency, in hours, that the device attempts to synchronize with the NTP servers. Values range from 0 to 168. With a value of 0, synchronization occurs only when the switch boots up.
ManualSyncRequest	Specifies that the device to immediately attempt to synchronize with the NTP servers.
LastSyncTime	Indicates the Coordinated Universal Time (UTC) when the device last synchronized with an NTP server. This is a read-only value.
LastSyncSourceInetAddress Type	Indicates the IP source address type of the NTP server with which this device last synchronized.
LastSyncSourceInetAddress	Indicates the IP source address of the NTP server with which this device last synchronized. This is a read-only value.
NextSyncTime	Indicates the UTC at which the next synchronization is scheduled.
PrimaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the primary server address. However, synchronization with the secondary server address can still occur.
SecondaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the secondary server address,
CurrentTime	Indicates the current switch UTC.

Configuring the local time zone using EDM

Use the following procedure to set a local time zone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **SNTP/Clock**.
3. In the work area, click the**Time Zone** tab.
4. In the **TimeZone** box, select the time zone offset.

5. In the **TimeZoneAcronym** dialog box, type a time zone acronym.
6. Click **Apply**.

Variable definitions

The following table describes the Time Zone screen fields.

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

Configuring daylight savings time using EDM

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

Prerequisites

Disable the summer time recurring feature.

Procedure steps

1. From the navigation tree, double-click Edit.
2. In the Edit tree, double-click **SNTP/Clock**.
3. In the work area, click the **Daylight Saving Time** tab.
4. In the **Offset** dialog box, type a value.
5. In the **TimeZoneAcronym** dialog box, type the time zone acronym.
6. In the **StartYear** dialog box, type a value.
7. In the **StartMonth** box, select a month.
8. In the **StartDay** dialog box, type a value.
9. In the **StartHour** box, select an hour.
10. In the **StartMinutes** dialog box, type a value.

11. In the **EndYear** dialog box, type a value.
12. In the **EndMonth** box, select a month.
13. In the **EndDay** dialog box, type a value.
14. In the **EndHour** box, select an hour.
15. In the **EndMinutes** dialog box, type a value.
16. Select the **Enabled** check box to enable daylight saving time for the switch.

    OR

    Clear the **Enabled** check box to disable daylight saving time for the switch.
17. Click **Apply** .

Variable definitions

Use the data in this table to configure the start and end of the daylight saving time period.

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

Variable	Value
EndHour	Specifies the hour of the particular day when to end the daylight savings time.
EndMinutes	Specifies the minute of the particular hour when to end the daylight savings time.
Enabled	Enables or disables day light saving time. **Important:** Before you enable daylight saving time, configure the feature attributes.

Configuring recurring daylight saving time using EDM

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

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **SNTP/Clock**.
3. In the work area, click the **SummerTimeRecurring** tab.
4. Select the **Recurring** check box to enable recurring daylight saving time for the switch.

   OR

   Clear the **Recurring** check box to disable recurring daylight saving time for the switch.
5. In **RecurringStartMonth**, make a selection from the drop-down list.
6. In **RecurringStartWeek**., click a button.
7. In **RecurringStartDay**, make a selection from the drop-down list.
8. In **RecurringStartHour**, make a selection from the drop-down list.
9. In the **RecurringStartMinute** dialog box, type a value from 0 to 59.
10. In **RecurringEndMonth**, make a selection from the drop-down list.
11. In **RecurringEndWeek**, click a button.
12. In **RecurringEndDay**, make a selection from the drop-down list.

13. In **RecurringEndHour**, make a selection from the drop-down list.
14. In the **RecurringEndMinute** dialog box, type a value from 0 to 59.
15. In the **RecurringOffset** dialog box, type a value from 1 to 1440.
16. On the tool bar, click **Apply**.

Variable definitions

Use the data in this table to configure recurring daylight saving time.

Variable	Value
Recurring	When selected, enables daylight saving time to recur yearly.
RecurringStartMonth	Specifies the month of each year you want recurring daylight savings time to start.
RecurringStartWeek	Specifies the week of the month you want recurring daylight savings time to start. Week 5 may not apply in certain years. In that case summer time start falls back to the 'last' option. For example: in a year where there is no Sunday in the fifth week of March, summer time will start on the last Sunday of March.
RecurringStartDay	Specifies the day of the particular month you want recurring daylight savings time to start.
RecurringStartHour	Specifies the hour of the particular day you want recurring daylight savings time to start.
RecurringStartMinute	Specifies the minutes of the particular hour you want recurring daylight savings time to start.
RecurringEndMonth	Specifies the month of each year you want recurring daylight savings time to end.
RecurringEndWeek	Specifies the week of the month you want recurring daylight savings time to end. Week 5 may not apply in certain years. In that case summer time start falls back to the 'last' option. For example: in a year where there is no Sunday in the fifth week of October, summer time will end on the last Sunday of October.

Variable	Value
RecurringEndDay	Specifies the day of the particular month you want recurring daylight savings time to end.
RecurringEndHour	Specifies the hour of the particular day you want recurring daylight savings time to end.
RecurringEndMinute	Specifies the minutes of the particular hour you want recurring daylight savings time to end.
RecurringOffset	Specifies the time in minutes by which you want to change the time when recurring daylight savings begins and ends. The offset is added to the current time when daylight saving time begins and subtracted from the current time when daylight saving time ends.

Viewing network topology information using EDM

Use this procedure to display network topology information.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **Topology**.
4. In the work area, click the **Topology** tab.
5. In the **Status** section, click a radio button..
6. Click **Apply** .

Variable definitions

Use the data in this table to help you understand the topology display.

Variable	Value
IpAddr	Indicates the IP address of the device.

Variable	Value
Status	Specifies whether Avaya topology is on (topOn) or off (topOff) for the device. The default value is topOn.
NmmLstChg	Indicates the value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent.
NmmMaxNum	Indicates the maximum number of entries in the NMM topology table.
NmmCurNum	Indicates the current number of entries in the NMM topology table.

Viewing the topology table using EDM

Use this procedure to display the topology table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **Topology**.
4. In the work area, click the **Topology Table** tab.

Variable definitions

Use the data in this table to help you understand the topology table display.

Variable	Value
Slot	Indicates the slot number in the chassis in which the topology message was received.
Port	Indicates the port on which the topology message was received.
IpAddr	Indicates the IP address of the sender of the topology message.
SegId	Indicates the segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	Indicates the MAC address of the sender of the topology message.

Variable	Value
ChassisType	Indicates the chassis type of the device that sent the topology message.
BkplType	Indicates the backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	Indicates the current state of the sender of the topology message. The choices are: • topChanged—Topology information has recently changed. • heartbeat—Topology information is unchanged. • new—The sending agent is in a new state.

LLDP configuration using EDM

Use the information in this section to configure and view Link Layer Discovery Protocol (LLDP) global and transmit properties for local and neighbor systems:

Configuring LLDP globally using EDM

Use the following procedure to configure LLDP transmit properties and view remote table statistics.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Globals** tab.
6. Edit global LLDP transmit properties.
7. Click **Apply** .

Variable definitions

The following table describes the Globals tab fields.

Variable	Value
lldpMessageTxInterval	the Indicates interval, in seconds, at which LLDP frames are transmitted on behalf of this LLDP agent.
lldpMessageTx HoldMultiplier	Indicates the time-to-live value expressed as a multiple of the object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, is expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval *lldpMessageTxHoldMultiplier) For example, if the value of lldpMessageTxInterval is 30, and the value of lldpMessageTxHoldMultiplier is 4, the value 120 is encoded in the TTL field in the LLDP header.
lldpReinitDelay	Indicates the lldpReinitDelay indicates the delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins.
lldpTxDelay	Indicates the lldpTxDelay indicates the delay (in seconds) between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The recommended value for the lldpTxDelay is set by the following formula: 1 <= lldpTxDelay <= (0.25 * lldpMessageTxInterval)
lldpNotificationInterval	Controls the transmission of LLDP notifications. The agent must not generate more than one lldpRemTablesChange notification-event in the indicated period, where a notification-event is the "transmission of a single notification PDU type to a list of notification destinations." If additional changes in lldpRemoteSystemsData object groups occur within the indicated throttling period, these trap-events must be suppressed by the agent. An NMS must periodically check the value of lldpStatsRemTableLastChangeTime to detect any missed lldpRemTablesChange notification-events, for example, due to throttling or transmission loss. If notification transmission is enabled for particular ports, the suggested default throttling period is 5 seconds.
RemTablesLast ChangeTime	Indicates the value of the sysUpTime object (defined in IETF RFC 3418) at the time an entry is created, modified, or deleted in tables associated with the lldpRemoteSystemsData objects, and all LLDP extension objects associated with remote systems. An

Variable	Value
	NMS can use this object to reduce polling of the lldpRemoteSystemsData objects.
RemTablesInserts	Indicates the number of times the complete set of information advertised by a particular MSAP is inserted into tables in lldpRemoteSystemsData and lldpExtensions objects. The complete set of information received from a particular MSAP is inserted into related tables. If partial information cannot be inserted for a reason such as lack of resources, all of the complete set of information is removed. This counter is incremented only once after the complete set of information is successfully recorded in all related tables. Any failures occurring during insertion of the information set, which result in deletion of previously inserted information, do not trigger any changes in lldpStatsRemTablesInserts because the insert is not completed yet or in lldpStatsRemTablesDeletes, because the deletion is only a partial deletion. If the failure is the result of a lack of resources, the lldpStatsRemTablesDrops counter is incremented once.
RemTablesDeletes	Indicates the number of times the complete set of information advertised by a particular MSAP is deleted from tables in lldpRemoteSystemsData and lldpExtensions objects. This counter is incremented only once when the complete set of information is completely deleted from all related tables. Partial deletions, such as a deletion of rows associated with a particular MSAP, from some tables, but not from all tables, are not allowed, and thus, do not change the value of this counter.
RemTablesDrops	Indicates the number of times the complete set of information advertised by a particular MSAP can not be entered into tables in lldpRemoteSystemsData and lldpExtensions objects because of insufficient resources.
RemTablesAgeouts	Indicates the number of times the complete set of information advertised by a particular MSAP is deleted from tables in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired. This counter is incremented only once when the complete set of information is completely invalidated (aged out) from all related tables. Partial aging, similar to deletion case, is not allowed, and thus, does not change the value of this counter.

Variable	Value
FastStartRepeatCount	Indicates the number of times the fast start LLDPDU is sent during the activation of the fast start mechanism defined by LLDP-MED.

Configuring port LLPD using EDM

Use the following procedure to configure the optional TLVs to include in the LLPDUs transmitted by each port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Port** tab.
6. To configure LLDP for a port, double-click a cell in a port row under a column heading.
7. Click **Apply** .

Variable definitions

The following table describes the Port tab fields.

Variable	Value
PortNum	Indicates the port number. This is a read-only cell.
AdminStatus	Indicates the administratively desired status of the local LLDP agent: • txOnly: the LLDP agent transmits LLDP frames on this port and does not store any information about the remote systems to which it is connected. • rxOnly: the LLDP agent receives but does not transmit LLDP frames on this port. • txAndRx: the LLDP agent transmits and receives LLDP frames on this port. • disabled: the LLDP agent does not transmit or receive LLDP frames on this port. If the port receives remote systems

Variable	Value
	information which is stored in other tables before AdminStatus is disabled, the information ages out.
NotificationEnable	Controls, on a per-port basis, whether notifications from the agent are enabled. • true: indicates that notifications are enabled • false: indicates that notifications are disabled.
TLVsTxEnable	Sets the optional Management TLVs to be included in the transmitted LLDPDUs: • portDesc: Port Description TLV • sysName: System Name TLV • sysDesc: System Description TLV • sysCap: System Capabilities TLV Note: The Local Management tab controls Management Address TLV transmission.
VLANTxEnable(dot1)	Specifies whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is included in the transmitted LLDPDUs.
TLVsTxEnable(dot3)	Sets the optional IEEE 802.3 organizationally defined TLVs to be included in the transmitted LLDPDUs: • macPhyConfigStatus: MAC/PHY configuration/status TLV • powerViaMDI: Power over MDI TLV • linkAggregation: Link Aggregation TLV • maxFrameSize: Maximum-frame-size TLV.
CapSupported(med)	Identifies which MED system capabilities are supported on the local system. This is a read-only cell.
TLVsTxEnable(med)	Sets the optional organizationally defined TLVs for MED devices to include in the transmitted LLDPDUs. • capabilities: Capabilities TLVs • networkPolicy: Network Policy TLVs • location: Emergency Communications System Location TLVs • extendedPSE: Extended PoE TLVs with PSE capabilities • inventory: Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, and Asset ID TLVs. The TLVs listed above are enabled by default.
NotifyEnable(med)	Enables or disables the topology change traps on this port.

Viewing LLDP TX statistics using EDM

Use the following procedure to display LLDP transmit statistics by port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click**802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **TX Stats** tab.

Variable definitions

The following table describes the TX Stats tab fields.

Variable	Value
PortNum	Indicates the port number
FramesTotal	Indicates the number of LLDP frames transmitted by this LLDP agent on the indicated port

Graphing LLDP transmit statistics using EDM

Use the following procedure to graph LLDP transmit statistics

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **TX Stats** tab.
6. In the table, select the port for which you want to display statistics.
7. On the toolbar, click **Graph**.

8. Highlight a data column to graph.
9. On the toolbar, click a graph button.

Viewing LLDP RX statistics using EDM

Use the following procedure to display LLDP receive statistics by port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **RX Stats** tab.

Variable definitions

The following table describes the RX Stats tab fields.

Variable	Value
PortNum	Indicates the port number.
FramesDiscardedTotal	Indicates the number of LLDP frames received on the port and discarded for any reason. This counter provides an indication that LLDP header formatting problems exist with the local LLDP agent in the sending system, or that LLDPDU validation problems exist with the local LLDP agent in the receiving system.
FramesErrors	Indicates the number of invalid LLDP frames received on the port, while the LLDP agent is enabled.
FramesTotal	Indicates the number of valid LLDP frames received on the port, while the LLDP agent is enabled.
TLVsDiscardedTotal	Indicates the number of LLDP TLVs discarded for any reason.
TLVsUnrecognizedTotal	Indicates the number of LLDP TLVs received on a given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001–111 1110) in Table 9.1

Variable	Value
	of IEEE 802.1ab-2004. An unrecognized TLV can be a basic management TLV from a later LLDP version.
AgeoutsTotal	Represents the number of age-outs that occurred on a given port. An age-out is "the number of times the complete set of information advertised by a particular MSAP is deleted from tables in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired." This counter is similar to lldpStatsRemTablesAgeouts, except that it is on a per-port basis. This enables NMS to poll tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems on the indicated port only. This counter is set to zero during agent initialization. When the admin status for a port changes from disabled to rxOnly, txOnly or txAndRx, the counter associated with the same port is reset to 0. The agent also flushes all remote system information associated with the same port. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, does not change the value of this counter.

Graphing LLDP RX statistics using EDM

Use the following procedure to graph LLDP receive statistics.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **RX Stats** tab.
6. In the table, select the port for which you want to display statistics.
7. On the toolbar, click **Graph**.
8. Highlight a data column to graph.
9. On the toolbar, click a graph button.

Viewing LLDP local system information using EDM

Use the following procedure to display LLDP properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Local System** tab.

Variable definitions

The following table describes the Local System tab fields.

Variable	Value
ChassisIdSubtype	Indicates the type of encoding used to identify the local system chassis: • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Indicates the chassis ID.
SysName	Indicates the local system name.
SysDesc	Indicates the local system description.
SysCapSupported	Indicates the system capabilities supported on the local system.
SysCapEnabled	Indicates the system capabilities that are enabled on the local system
DeviceClass	Indicates the MED device class.

Variable	Value
HardwareRev	Indicates the vendor-specific hardware revision string.
FirmwareRev	Indicates the vendor-specific firmware revision string.
SoftwareRev	Indicates the vendor-specific software revision string.
SerialNum	Indicates the vendor-specific serial number.
MfgName	Indicates the vendor-specific manufacturer name.
ModelName	Indicates the vendor-specific model name.
AssetID	Indicates the vendor-specific asset tracking identifier
DeviceType	Defines the type of Power-via-MDI (PoE). • pseDevice • pdDevice • none
PDPowerSource	Defines the type of PD Power Source.
PDPowerReq	Specifies the value of the power required in 0.1 W increments by a PD.
PSEPowerSource	Defines the type of PSE Power Source (primary or back-up).
PDPowerPriority	Defines the Powered Device (PD) power priority. • critical • high • low

Viewing LLDP local port information using EDM

Use the following procedure to display LLDP port properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.

4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Local Port** tab.

Variable definitions

The following table describes the Local Port tab fields.

Variable	Value
PortNum	Indicates the port number.
PortIdSubtype	Indicates the type of port identifier encoding used in the associated PortId object. • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local.
PortId	Indicates the string value used to identify the port component associated with a given port in the local system.
PortDesc	Indicates the string value used to identify the 802 LAN station port description associated with the local system. If the local agent supports IETF RFC 2863, the PortDesc object has the same value as the ifDescr object.

Viewing LLDP local management information using EDM

Use the following procedure to display LLDP management properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostic tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Local Management** tab.

Variable definitions

The following table describes the Local Management tab fields.

Variable	Value
AddrSubtype	Indicates the type of management address identifier encoding used in the associated Addr object.
Addr	Indicates the string value used to identify the management address component associated with the local system. This address is used to contact the management entity. The switch supports IPv4 and IPv6 management addresses. **Note:** If you configure both IPv4 and IPv6 management addresses, the switch displays each on a separate row.
AddrLen	Indicates the total length of the management address subtype and the management address fields in LLDPDUs transmitted by the local LLDP agent. The management address length field is needed so that the receiving systems that do not implement SNMP are not required to implement the family numbers/ address length equivalency table to decode the management address.
AddrIfSubtype	Identifies the numbering method used to define the interface number associated with the remote system. • unknown • ifIndex • systemPortNumber
AddrIfId	Indicates the integer value used to identify the interface number of the management address component associated with the local system.
AddrOID	Indicates the value used to identify the type of hardware component or protocol entity associated with the management address advertised by the local system agent.
AddrPortsTxEnable	Specifies the ports on which the local system management address TLVs are transmitted in the LLPDUs.

Enabling or disabling LLDP Management Address TLV transmission using EDM

Use the following procedure to enable or disable the transmission of Management Address TLVs on the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Local Management** tab.
6. Double-lick the cell in the **AddPortsTxEnable** column for an IPv4 or IPv6 row.
7. To enable the transmission of Management Address TLVs, select one or more port numbers.

   OR

   To disable the transmission of Management Address TLVs, deselect one or more port numbers.
8. Click **Ok**.
9. On the toolbar, click **Apply**.

Viewing LLDP neighbor information using EDM

Use the following procedure to display LLDP properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Neighbor** tab.

Variable definitions

The following table describes the Neighbor tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ChassisIdSubtype	Indicates the type of encoding used to identify the remote system chassis: • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local.
ChassisId	Indicates the remote chassis ID.
SysCapSupported	Identifies the system capabilities supported on the remote system.
SysCapEnabled	Identifies the system capabilities that are enabled on the remote system.
SysName	Indicates the remote system name.
SysDesc	Indicates the remote system description.
PortIdSubtype	Indicates the type of encoding used to identify the remote port. • interfaceAlias • portComponent • macAddress • networkAddress

Variable	Value
	• interfaceName • agentCircuitId • local
PortId	Indicates the remote port ID.
PortDesc	Indicates the remote port description.

Viewing LLDP neighbor management information using EDM

Use the following procedure to display LLDP management properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostic tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Neighbor Mgmt Address** tab.

Variable definitions

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
AddrSubtype	Indicates the type of encoding used in the associated Addr object.
Addr	Indicates the management address associated with the remote system. The switch supports IPv4 and IPv6 management addresses.

Variable	Value
	Note: If you configure both IPv4 and IPv6 management addresses, the switch displays each on a separate row.
AddrIfSubtype	Indicates the numbering method used to define the interface number associated with the remote system. • unknown • ifIndex • systemPortNumber
AddrIfId	Indicates the integer value used to identify the interface number of the management address component associated with the remote system.
AddrOID	Indicates the value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.

Viewing LLDP unknown TLV information using EDM

Use the following procedure to display details about unknown TLVs received on the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Unknown TLV** tab.

Variable definitions

The following table describes the Unknown TLV tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.

Variable	Value
LocalPortNum	Indicates the local port which receives the remote system information.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
UnknownTLVType	Indicates the value extracted from the type field of the unknown TLV.
UnknownTLVInfo	Indicates the value extracted from the value field of the unknown TLV.

Viewing LLDP organizational defined information using EDM

Use the following procedure to display organizational-specific properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Organizational Defined Info** tab.

Variable definitions

The following table describes the Organizational Defined Info tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port that receives the remote system information.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.

Variable	Value
OrgDefInfoOUI	Indicates the Organizationally Unique Identifier, as defined in IEEE 802-2001, is a 24 bit (three octets) globally unique assigned number referenced by various standards, of the information received from the remote system.
OrgDefInfoSubtype	Indicates the integer value used to identify the subtype of the organizationally defined information received from the remote system. The subtype value is required to identify different instances of organizationally defined information that cannot be retrieved without a unique identifier that indicates the particular type of information in the information string.
OrgDefInfoIndex	Represents an arbitrary local integer value used by this agent to identify a particular unrecognized organizationally defined information instance, unique only for the OrgDefInfoOUI and lldpRemOrgDefInfoSubtype of the same remote system. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot. It is unlikely that the lldpRemOrgDefInfoIndex will wrap between reboots.
OrdDefInfo	Indicates the string value used to identify the organizationally defined information of the remote system. The encoding for this object is the same as that defined for SnmpAdminString TC.

LLDP Port dot1 configuration using EDM

Use the information in this section to configure and view IEEE 802.1 LLDP information.

Viewing local VLAN Id information using EDM

Use the following procedure to display LLDP VLAN ID properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.

3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Local VLAN Id** tab.

Variable definitions

The following table describes the Local VLAN Id tab fields.

Variable	Value
PortNum	Indicates the port number.
VlanId	Indicates the local port VLAN ID. A value of zero is used if the system does not know the PVID.

Viewing LLDP local protocol VLAN information using EDM

Use the following procedure to display LLDP local protocol VLAN properties for the local system and to enable or disable the transmission of this information from a specified port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Local Protocol VLAN** tab.
6. To select a port to edit, click the port row.
7. In the port row, double-click the cell in the **ProtoVlanTxEnable** column.
8. Select a value from the list—**true** to enable transmitting local port and protocol VLAN information from the port, or **false** to disable transmitting local port and protocol VLAN information from the port.
9. Click **Apply** .

Variable definitions

The following table describes the Local Protocol VLAN tab fields.

Variable	Value
PortNum	Indicates the port number.
ProtoVlanId	Indicates the ID of the port and protocol VLANs associated with the local port. A value of zero is used if the system does not know the protocol VLAN ID (PPVID).
ProtoVlanSuported	Indicates whether the local port supports port and protocol VLANs.
ProtoVlanEnabled	Indicates whether the port and protocol VLANs are enabled on the local port.
ProtoVlanTxEnable	Specifies whether the corresponding local port and protocol VLAN information are transmitted from the port.

Viewing LLDP local VLAN name information using EDM

Use the following procedure to display LLDP VLAN Name properties for the local system and to enable or disable the transmission of this information from a specified port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Local VLAN Name** tab.
6. To select a port to edit, click the port row.
7. In the port row, double-click the cell in the **VlanNameTxEnable** column.
8. Select a value from the list—**true** to enable transmitting local VLAN name information from the port, or **false** to disable transmitting local VLAN name information from the port.
9. Click **Apply** .

Variable definitions

The following table describes the Local VLAN Name tab fields.

Variable	Value
PortNum	Indicates the port number.
VlanId	Indicates the integer value used to identify the IEEE 802.1Q VLAN IDs with which the given port is compatible.
VlanName	Indicates the string value used to identify the VLAN name identified by the VLAN ID associated with the given port on the local system. This object contains the value of the dot1QVLANStaticName object (defined in IETF RFC 2674) identified with the given lldpXdot1LocVlanId.
VlanNameTxEnable	Specifies whether the corresponding Local System VLAN name instance is transmitted from the port.

Viewing LLDP local protocol information using EDM

Use the following procedure to display LLDP protocol properties for the local system and to enable or disable the transmission of this information from a specified port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Local Protocol** tab.
6. To select a port to edit, click the port row.
7. In the port row, double-click the cell in the **VlanNameTxEnable** column.
8. Select a value from the list—**true** to enable transmitting local protocol information from the port, or **false** to disable transmitting local protocol information from the port.
9. Click **Apply** .

Variable definitions

The following table describes the Local Protocol tab fields.

Variable	Value
PortNum	Indicates the port number.
ProtocolIndex	Indicates the arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	Indicates the octet string value used to identify the protocols associated with the given port of the local system.
ProtocolTxEnable	Specifies whether the corresponding Local System Protocol Identity instance is transmitted on the port.

Viewing LLDP neighbor VLAN ID information using EDM

Use the following procedure to view the LLDP VLAN ID properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Neighbor VLAN Id** tab.

Variable definitions

The following table describes the Neighbor VLAN ID tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
VlanId	Indicates the port VLAN identifier associated with the remote system. If the remote system does not know

Variable	Value
	the PVID or does not support port-based VLAN operation, the value is zero.

Viewing LLDP neighbor protocol VLAN information using EDM

Use the following procedure to display LLDP protocol VLAN properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Neighbor Protocol VLAN** tab.

Variable definitions

The following table describes the Neighbor Protocol VLAN tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ProtoVlanId	Indicates the ID of the port and protocol VLANs associated with the remote port. A value of zero is used if the system does not know the protocol VLAN ID (PPVID).
ProtoVlanSuported	Indicates whether the remote port supports port and protocol VLANs.
ProtoVlanEnabled	Indicates whether the port and protocol VLANs are enabled on the remote port.

Viewing LLDP neighbor VLAN name information using EDM

Using the following procedure to display LLDP VLAN name properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Neighbor VLAN Name** tab.

Variable definitions

The following table describes the Neighbor VLAN Name tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
VlanId	Indicates the integer value used to identify the IEEE 802.1Q VLAN IDs with which the remote port is compatible.
VlanName	Indicates the VLAN name identified by the VLAN ID associated with the remote system.

Viewing LLDP neighbor protocol information using EDM

Use the following procedure to display LLDP protocol properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Neighbor Protocol** tab.

Variable definitions

The following table describes the Neighbor Protocol tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ProtocolIndex	Represents an arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	Indicates the protocols associated with the remote port.

LLDP Port dot3 configuration using EDM

Use the information in this section to configure and view IEEE 802.3 LLDP information.

Viewing LLDP local port auto-negotiation information using EDM

Use the following procedure to display LLDP auto-negotiation properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Local Port Auto-negotiation** tab.

Variable definitions

The following table describes the Local Port Auto-negotiation tab fields.

Variable	Value
PortNum	Indicates the port number.
AutoNegSupported	Indicates whether the local port supports Auto-negotiation.
AutoNegEnabled	Indicates whether Auto-negotiation is enabled on the local port.
AutoNegAdvertisedCap	Contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the local port on the system.
OperMauType	Indicates the value that indicates the operational MAU type of the given port on the local system.

Viewing LLDP local PoE information using EDM

Use the following procedure to display LLDP PoE properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.

4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Local PoE** tab.

Variable definitions

The following table describes the Local PoE tab fields.

Variable	Value
PortNum	Indicates the port number.
PowerPortClass	Indicates the port Class of the local port.
PowerMDISupported	Indicates whether MDI power is supported on the local port.
PowerMDIEnabled	Indicates whether MDI power is enabled on the local port.
PowerPairControlable	Indicates the value derived from the value of the pethPsePortPowerPairsControlAbility object (defined in IETF RFC 3621), this value is used to indicate whether pair selection can be controlled on the local port.
PowerPairs	Contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the local port: • signal • spare
PowerClass	Contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the local port: • class0 • class1 • class2 • class3 • class4

Viewing Local Link Aggregate tab using EDM

Use the following procedure to display LLDP link aggregation properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Local Link Aggregate** tab.

Variable definitions

The following table describes the Local Link Aggregate tab fields.

Variable	Value
PortNum	Indicates the port number.
LinkAggStatus	Specifies the link aggregation capabilities and the current aggregation status of the link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation. If the port is not in a link aggregation state or does not support link aggregation, this value is set to zero.

Viewing LLDP local maximum frame information using EDM

Use the following procedure to display LLDP maximum frame size properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Local Max Frame** tab.

Variable definitions

The following table describes the Local Max Frame tab fields.

Variable	Value
PortNum	Indicates the port number.
MaxFrameSize	Indicates the maximum frame size for the port.

Viewing LLDP neighbor port auto-negotiation information using EDM

Use the following procedure to display LLDP auto-negotiation properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Neighbor Port Auto-negotiation** tab.

Variable definitions

The following table describes the Neighbor Port Auto-negotiation tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.

Variable	Value
AutoNegSupported	Indicates the truth value used to indicate whether the given port (associated with a remote system) supports Auto-negotiation.
AutoNegEnabled	Indicates whether Auto-negotiation is enabled on the remote port.
AutoNegAdvertisedCap	Contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the remote port.
OperMauType	Indicates the value that indicates the operational MAU type of the given port on the remote system.

Viewing LLDP neighbor PoE information using EDM

Use the following procedure to display LLDP PoE properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Neighbor PoE** tab.

Variable definitions

The following table describes the Neighbor PoE tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PowerPortClass	Indicates the port Class of the remote port.

Variable	Value
PowerMDISupported	Indicates whether MDI power is supported on the remote port.
PowerMDIEnabled	Indicates whether MDI power is enabled on the remote port.
PowerPairControlable	Indicates the value derived from the value of the pethPsePortPowerPairsControlAbility object (defined in IETF RFC 3621), this value is used to indicate whether pair selection can be controlled on the remote port.
PowerPairs	Contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the remote port. • signal • spare
PowerClass	Contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the remote port. • class0 • class1 • class2 • class3 • class4

Viewing LLDP neighbor link aggregation information using EDM

Use the following procedure to display LLDP link aggregation properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Neighbor Link Aggregate** tab.

Variable definitions

The following table describes the Neighbor Link Aggregate tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
LinkAggStatus	Specifies the link aggregation capabilities and the current aggregation status of the remote link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation. If the port is not in a link aggregation state or does not support link aggregation, this value is set to zero.

Viewing LLDP neighbor maximum frame information using EDM

Use the following procedure to display LLDP maximum frame size properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Neighbor Max Frame** tab.

Variable definitions

The following table describes the Neighbor Max Frame tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
MaxFrameSize	Indicates the maximum frame size for the remote port.

LLDP Port MED configuration using EDM

Use the information in this section to configure and view LLDP Media Endpoint Devices (MED) information.

LLDP MED policy management using EDM

Use the information in this section to view, create, and edit LLDP MED policies for the switch.

Viewing LLDP MED policies using EDM

Use this procedure to view LLDP MED policy properties for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.

Variable definitions

Use the data in the following table to help you understand the LLDP MED local policy display.

Field	Description
PortNum	Indicates the port number
PolicyAppType	Shows the policy application type.
PolicyVlanID	Indicates the extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the local port. The default value is 6.
PolicyDscp	Contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the given port on the local system. The default value is 46.
PolicyTagged	Indicates whether the application is using a tagged VLAN, untagged VLAN, or does not support a port based VLAN operation.

Creating LLDP MED policies using EDM

Use this procedure to create a new LLDP MED policy for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.
6. Click **Insert** .
7. To select a port to create a policy for, click the **PortNum** elipsis.
8. Click **Ok** .
9. In the **PolicyAppType** section, select one or both checkboxes.
10. To select a VLAN identifier for the selected port, click the **PolicyVlanID** elipsis.
11. Click **Ok** .

12. Double-click the **PolicyPriority** field.
13. Type a priority value.
14. Double-click the **PolicyDscp** field.
15. Type a DSCP value.
16. To use a tagged VLAN, select the **PolicyTagged** checkbox.

    OR

    To use an untagged VLAN, clear the **PolicyTagged** checkbox.
17. Click **Insert** .

Variable definitions

Use the data in the following table to create a new LLDP MED policy for the local system.

Field	Description
PortNum	Specifies the port on which to configure LLDP MED policies.
PolicyAppType	Specifies the policy application type. • voice—selects the voice network policy • voiceSignaling—selects the voice signalling network policy
PolicyVlanID	Specifies the VLAN identifier for the selected port or ports. Values range from 1–4094. If you select priority tagged frames, the system recognizes only the 802.1p priority level and uses a value of 0 for the VLAN ID of the ingress port.
PolicyPriority	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. Values range from 0–7. The default value is 6.
PolicyDscp	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63. The default value is 46.
PolicyTagged	Specifies the type of VLAN tagging to apply on the selected switch port or ports. • when selected—uses a tagged VLAN • when cleared—uses an untagged VLAN or does not support port-based VLANs.

Field	Description
	If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.

Editing LLDP MED policies using EDM

Use this procedure to edit a previously configured LLDP MED policy for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. To select a policy to edit, click the **PortNum**.
6. In the policy row, double-click the cell in the**PolicyVlanID** column.
7. Select a VLAN from the list.
8. Click **Ok** .
9. In the policy row, double-click the cell in the**PolicyPriority** column.
10. Edit the policy priority value.
11. In the policy row, double-click the cell in the**PolicyDscp** column.
12. Edit the policy DSCP value.
13. In the policy row, double-click the cell in the**PolicyTagged** column.
14. Select a value from the list.
15. Click **Apply** .

Variable definitions

Use the data in the following table to edit a previously configured LLDP MED policy for the local system.

Variable	Value
PortNum	Indicates the port on which to configure LLDP MED policies. This is a read-only cell.
PolicyAppType	Indicates the policy application type. This is a read-only cell. • voice— voice network policy • voiceSignaling— voice signalling network policy

Variable	Value
PolicyVlanID	Specifies the VLAN identifier for the selected port or ports. Values range from 1–4094. If you select priority tagged frames, the system recognizes only the 802.1p priority level and uses a value of 0 for the VLAN ID of the ingress port.
PolicyPriority	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. Values range from 0–7. The default value is 6.
PolicyDscp	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63. The default value is 46.
PolicyTagged	Specifies the type of VLAN tagging to apply on the selected switch port or ports. • true—uses a tagged VLAN • false—uses an untagged VLAN or does not support port-based VLANs. If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.

Deleting LLDP MED policies using EDM

Use this procedure to delete a LLDP MED policy.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.
6. To select a policy to delete, click the **PortNum**.
7. Click **Delete** .

Local location information management using EDM

Use the information in this section to view and add local location information for remote network devices connected to a switch or stack.

Viewing device location information using EDM

Use this procedure to display local location information for remote network devices connected to a switch or stack.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Local Location** tab.

Variable definitions

Use the data in the following table to help you understand the remote device local location information display.

Field	Description
PortNum	Identifies the port number of the local system to which the remote device is connected.
LocationSubtype	Indicates the location subtype advertised by the remote device. • unknown • coordinateBased—location information is based on geographical coordinates of the remote device • civicAddress—location information is based on the civic address of the remote device • elin—location information is based on the Emergency Location Information Number (ELIN) of the remote device
LocationInfo	Displays local location information advertised by the remote device. The information displayed in this cell is directly associated with the location subtype value.

Adding ELIN based device location information using EDM

Use this procedure to add information to the local location table for remote network devices connected to a switch or stack, based on an Emergency Location Information Number (ELIN).

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Local Location** tab.
6. In the port row with **elin** as the location subtype, double-click the cell in the **LocationInfo** column.
7. Type an alphanumeric value from 10 to 25 characters in length.
8. Click **Apply** .

Adding coordinate and civic address based device location information using EDM

Use this procedure to add local location information to the local location table for remote network devices connected to a switch or stack, based on geographical coordinates and a civic address.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Local Location** tab.
6. To add location information based on geographical coordinates for the remote device, click the **coordinateBased** cell in the LocationSubtype column for a port.
7. To add location information based on the civic address for the remote device, click the **civicAddress** cell in the LocationSubtype column for a port.
8. Click **Location Detail**.
9. Insert the local location information for the remote device.
10. Click **Ok** .
11. Click **Apply** .

Variable definitions

Use the data in the following table to add coordinate-based location information for the remote device.

Field	Description
Latitude	Specifies the latitude in degrees, and its relation to the equator (North or South).
Longitude	Specifies the longitude in degrees, and its relation to the prime meridian (East or West).
Altitude	Specifies the altitude, and the units of measurement used (meters or floors).
Map Datum	Specifies the map reference datum. Values include: • WGS84—World Geodesic System 1984, Prime Meridian Name: Greenwich • NAD83/NAVD88—North American Datum 1983/ North American Vertical Datum of 1988 • NAD83/MLLW—North American Datum 1983/ Mean Lower Low Water

Viewing local PoE PSE information using EDM

Use this procedure to display LLDP PoE PSE information for the local system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Local PoE PSE** tab.

Variable definitions

The following table describes the Local PoE PSE tab fields.

Field	Description
PortNum	Indicates the port number.
PSEPortPowerAvailable	Contains the value of the power available (in units of 0.1 watts) from the PSE through this port.
PSEPortPDPriority	Indicates the PD power priority that is advertised on this PSE port: • unknown: priority is not configured or known by the PD • critical: the device advertises its power priority as critical, see RFC 3621 • high: the device advertises its power priority as high, see RFC 3621 • low: the device advertises its power priority as low, see RFC 3621

Viewing neighbor capabilities using EDM

Use this procedure to display LLDP capabilities for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor Capabilities** tab.

Variable definitions

The following table describes the Neighbor Capabilities tab fields.

Field	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.

Field	Description
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
CapSupported	Identifies the MED system capabilities supported on the remote system.
CapCurrent	Identifies the MED system capabilities that are enabled on the remote system.
DeviceClass	Indicates the remote MED device class.

Viewing neighbor policies using EDM

Use this procedure to display LLDP policy information for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor Policy** tab.

Variable definitions

The following table describes the Neighbor Policy tab fields.

Field	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.

Field	Description
PolicyAppType	Shows the policy application type.
PolicyVlanID	Indicates the extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and that the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the remote system connected to the port.
PolicyDscp	Contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the remote system connected to the port.
PolicyUnknown	Indicates whether the network policy for the specified application type is currently unknown or defined.
PolicyTagged	Indicates whether the application is using a tagged VLAN, untagged VLAN, or does not support a port based VLAN operation.

Neighbor location information management using EDM

Use the information in this section to view and add neighbor location information for network devices connected to a switch or stack.

Viewing neighbor location information using EDM

Use this procedure to display LLDP neighbor location information.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor Location** tab.

Variable definitions

The following table describes the Neighbor Location tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
LocationSubtype	Indicates the location subtype advertised by the remote device: • unknown • coordinateBased • civicAddress • elin
LocationInfo	Indicates the location information advertised by the remote device. The parsing of this information depends on the location subtype.

Adding coordinate-based neighbor location information using EDM

Use this procedure to add coordinate-based location information to the neighbor location table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor Location** tab.
6. In the table, select a location with the **LocationSubtype** listed as **coordinateBased**.
7. On the toolbar, click the **Location Details** button.

   The Insert Local Location dialog box appears.

8. Click **Close** to close the dialog box.
9. Click **Apply** .

Adding civic address location information using EDM

Use this procedure to add civic address-based location information to the neighbor location table.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor Location** tab.
6. In the table, select a location with the **LocationSubtype** listed as **civicAddress**.
7. On the toolbar, click the **Location Details** button.

   The Insert Local Location dialog box appears.
8. Click **Close** to close the dialog box.
9. Click **Apply** .

Viewing neighbor PoE information using EDM

Use this procedure to display LLDP PoE properties for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor PoE** tab.

Variable definitions

The following table describes the Neighbor PoE tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PoeDeviceType	Defines the type of Power-via-MDI (Power over Ethernet) advertised by the remote device: • pseDevice: indicates that the device is advertised as a Power Sourcing Entity (PSE). • pdDevice: indicates that the device is advertised as a Powered Device (PD). • none: indicates that the device does not support PoE.

Viewing neighbor PoE PSE information using EDM

Use this procedure to display LLDP PoE PSE information for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor PoE PSE** tab.

Variable definitions

The following table describes the Neighbor PoE PSE tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PSEPowerAvailable	Specifies the power available (in units of 0.1 watts) from the PSE connected remotely to this port.
PSEPowerSource	Defines the type of PSE Power Source advertised by the remote device. • primary: indicates that the device advertises its power source as primary. • backup: indicates that the device advertises its power source as backup.
PSEPowerPriority	Specifies the priority advertised by the PSE connected remotely to the port: • critical: indicates that the device advertises its power priority as critical, see RFC 3621. • high: indicates that the device advertises its power priority as high, see RFC 3621. • low: indicates that the device advertises its power priority as low, see RFC 3621.

Viewing neighbor PoE PD information using EDM

Use this procedure to display LLDP PoE PD information for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.

4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor PoE PD** tab.

Variable definitions

The following table describes the Neighbor PoE PD tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PDPowerReq	Specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD) connected remotely to the port.
PDPowerSource	Defines the type of Power Source advertised as being used by the remote device: • fromPSE: indicates that the device advertises its power source as received from a PSE. • local: indicates that the device advertises its power source as local. • localAndPSE: indicates that the device advertises its power source as using both local and PSE power.
PDPowerPriority	Defines the priority advertised as being required by the PD connected remotely to the port: • critical: indicates that the device advertises its power priority as critical, see RFC 3621. • high: indicates that the device advertises its power priority as high, see RFC 3621. • low: indicates that the device advertises its power priority as low, see RFC 3621.

Viewing neighbor inventory using EDM

Use this procedure to display LLDP inventory information for the remote system.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. On the work area, click the **Neighbor Inventory** tab.

Variable definitions

The following table describes the Neighbor Inventory tab fields.

Variable	Value
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
HardwareRev	Indicates the vendor-specific hardware revision string as advertised by the remote device.
FirmwareRev	Indicates the vendor-specific firmware revision string as advertised by the remote device.
SoftwareRev	Indicates the vendor-specific software revision string as advertised by the remote device.
SerialNum	Indicates the vendor-specific serial number as advertised by the remote device.

Variable	Value
MfgName	Indicates the vendor-specific manufacturer name as advertised by the remote device.
ModelName	Indicates the vendor-specific model name as advertised by the remote device.
AssetID	Indicates the vendor-specific asset tracking identifier as advertised by the remote device.

Enabling or disabling Avaya TLV transmit flags using EDM

Use this procedure to enable or disable the transmission of optional proprietary Avaya TLVs from switch ports to Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Port Config** tab.
6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **TLVsTxEnable** column.
8. Select a checkbox to enable a TLV.

   OR

   Clear a checkbox to disable a TLV.
9. Click **Ok**.
10. On the toolbar, click **Apply**.

Variable definition

Variable	Value
poeConservationLevel	Enables or disables the TLV for requesting a specific power conservation level for an Avaya IP phone connected to the switch port.

Variable	Value
	Important: Only Ethernet ports on switches that support PoE can request a specific power conservation level for an Avaya IP phone.
callServer	Enables or disables the TLV for advertising call server IPv4 addresses to an Avaya IP phone connected to the switch port.
fileServer	Enables or disables the TLV for advertising file server IPv4 addresses to an Avaya IP phone connected to the switch port.
framingTlv	Enables or disables the frame tagging TLV for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Viewing the Avaya TLV transmit flag status using EDM

Use this procedure to display the status of transmit flags for switch ports on which Avaya IP phone support TLVs are configured.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Port Config** tab.

Variable definition

Variable	Value
poeConservationLevel	When displayed, indicates that the TLV for requesting a specific power conservation level for an Avaya IP phone is enabled on the switch port. **Important:** Only Ethernet ports on switches that support PoE can request a specific power conservation level for an Avaya IP phone.
callServer	When displayed, indicates that call server IPv4 address advertisement to an Avaya IP phone is enabled on the switch port.

Variable	Value
fileServer	When displayed, indicates that file server IPv4 address advertisement to an Avaya IP phone is enabled on the switch port.
framingTlv	When displayed, indicates that frame tagging is enabled on the port, for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Configuring the PoE conservation level request TLV using EDM

Use this procedure to request a specific power conservation level for an Avaya IP phone connected to a switch port.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local Port** tab.
6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **PoeConsLevelRequest** column.
8. Type a value in the box.
9. On the toolbar, click **Apply**.

Variable definition

Variable	Value
PoeConsLevelRequest	Specifies the power conservation level to request for a vendor specific PD. Values range from 0 to 255. With the default value of 0, the switch does not request a power conservation level for an Avaya IP phone connected to the port.

Configuring the 802.1Q framing TLV using EDM

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local Port** tab.
6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **Dot1QFramingRequest** column.
8. Select a value from the list.
9. On the toolbar, click **Apply**.

Variable definition

Variable	Value
Dot1QFramingRequest	Specifies the frame tagging mode. Values include: • tagged—frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • non-tagged—frames are not tagged with 802.1Q priority. • auto—an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. The default tagging mode is auto.

Viewing the PoE conservation level request and 802.1Q framing TLV configuration using EDM

Use this procedure to display the configuration status of the PoE conservation level request and 802.1Q framing TLVs that the switch can transmit to Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local Port** tab.

Variable definition

Variable	Value
Dot1QFramingRequest	Displays the frame tagging mode. Values include: • tagged—frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • non-tagged—frames are not tagged with 802.1Q priority. • auto—an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. The default tagging mode is auto.
PoeConsLevelRequest	Specifies the power conservation level to request for a vendor specific PD. Values range from 0 to 255. With the default value of 0, the switch does not request a power conservation level for an Avaya IP phone connected to the port.

Configuring the switch call server IP address TLV using EDM

Use this procedure to define the local call server IP addresses that switch ports can advertise to Avaya IP phones.

You can define IP addresses for a maximum of 8 local call servers.

Important:
The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local Call Servers** tab.
6. To select a port, click the **CallServerNum**.
7. In the port row, double-click the cell in the **CallServerAddress** column.
8. Type an IP address in the box.
9. On the toolbar, click **Apply**.

Variable definition

Variable	Value
CallServerNum	Displays the call server number.
CallServerAddressType	Displays the call server IP address type.
CallServerAddress	Defines the local call server IP address to advertise.

Viewing the switch call server IP address TLV configuration using EDM

Use this procedure to display information about the defined local call server IP addresses that switch ports can advertise to Avaya IP phones.

Important:

The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local Call Servers** tab.

Variable definition

Variable	Value
CallServerNum	Displays the call server number.
CallServerAddressType	Displays the call server IP address type.
CallServerAddress	Displays the defined call server IP address.

Configuring the switch file server IP address TLV using EDM

Use this procedure to define the local file server IP addresses that switch ports can advertise to Avaya IP phones.

You can define IP addresses for a maximum of 4 local call servers.

Note:

If your Avaya IP Handset uses SIP, 802.1AB (LLDP) TLVs do not provide all information for the IP Phone. You must specify a file server IP address TLV so the IP phone can download the SIP configuration information, because the IP Phone retrieves information related to the SIP domain, port number and transport protocol from the file server.

Important:
The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local File Servers** tab.
6. To select a port, click the **FileServerNum**.
7. In the port row, double-click the cell in the **FileServerAddress** column.
8. Type an IP address in the box.
9. On the toolbar, click **Apply**.

Variable definition

Variable	Value
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Defines file server IP address to advertise.

Viewing the switch file server IP address TLV configuration using EDM

Use this procedure to display information about the defined local file server IP addresses that switch ports can advertise to Avaya IP phones.

Important:
The switch does not support the advertisement of IPv6 addresses to Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Local File Servers** tab.

Variable definition

Variable	Value
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Displays the defined file server IP address.

Viewing Avaya IP phone power level TLV information using EDM

Use this procedure to display power level information received on switch ports from an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor Devices** tab.

Variable definition

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
CurrentConsLevel	Displays the PoE conservation level configured on the Avaya IP phone connected to the switch port.
TypicalPower	Displays the average power level used by the Avaya IP phone connected to the switch port.
MaxPower	Displays the maximum power level for the Avaya IP phone connected to the switch port.

Viewing remote call server IP address TLV information using EDM

Use this procedure to display call server IP address information received on switch ports from an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor Call Servers** tab.

Variable definition

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PortCallServerAddressType	Displays the call server IP address type used by the Avaya IP phone connected to the switch port.
PortCallServerAddress	Displays the call server IP address used by the Avaya IP phone connected to the switch port.

Viewing remote file server IP address TLV information using EDM

Use this procedure to display file server IP address information received on switch ports from an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor File Servers** tab.

Variable definition

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PortFileServerAddressType	Displays the file server IP address type used by the Avaya IP phone connected to the switch port.
PortFileServerAddress	Displays the file server IP address used by the Avaya IP phone connected to the switch port.

Viewing PoE conservation level support TLV information using EDM

Use this procedure to display PoE conservation level information received on switch ports from an Avaya IP phone.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor PoE** tab.

Variable definition

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.
PoeConsLevelValue	Displays the PoE conservation level supported by the Avaya IP phone connected to the switch port.

Viewing remote 802.1Q Framing TLV information using EDM

Use this procedure to display Layer 2 frame tagging mode information received on switch ports from connected Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor Dot1Q** tab.

Variable definition

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected Avaya IP phone.

Variable	Value
Dot1QFraming	Displays the Layer 2 frame tagging mode for the Avaya IP phone connected to the switch port. Values include: • tagged—frames are tagged based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. • non-tagged—frames are not tagged with 802.1Q priority. • auto—an attempt is made to tag frames based on the tagging value the Avaya IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged. • The default tagging mode is auto.

Viewing remote IP TLV information using EDM

Use this procedure to display IP address configuration information received on switch ports from connected Avaya IP phones.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Avaya**.
5. In the work area, click the **Neighbor IP Phone** tab.

Variable definition

Variable	Value
TimeMark	Displays the time the latest TLV-based information is received from an Avaya IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.

Variable	Value
Index	Displays a unique identifier for the connected Avaya IP phone.
PortPhoneAddressType	Displays the IP address type for the Avaya IP phone connected to the switch port.
PortPhoneAddress	Displays the IP address for the Avaya IP phone connected to the switch port.
PortPhoneAddressMask	Displays the IP address subnet mask for the Avaya IP phone connected to the switch port.
PortPhoneGatewayAddress	Displays gateway the IP address for the Avaya IP phone connected to the switch port.

Global AES configuration using EDM

Use the information in this section to configure Avaya Energy Saver (AES) for an single switch or a stack.

Enabling global AES using EDM

Use the following procedure to enable energy saving for the switch.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **EnergySaverEnabled** check box.
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 describes the Energy Saver Globals tab fields.

Variable	Value
EnergySaverEnabled	Enables or disables energy saving for the switch.
PoePowerSavingEnabled	Enables or disables AES PoE power save mode for the switch.
EfficiencyModeEnabled	Enables or disables AES efficiency mode for the switch.
EnergySaverActive	Activates or deactivates the Avaya Energy Saver.

Disabling global AES using EDM

Use the following procedure to disable energy saving for the switch.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **EnergySaverEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

Enabling global AES PoE power save mode using EDM

Use the following procedure to enable AES PoE power save mode for the switch.

When enabled, AES PoE power save mode provides the capability to control power consumption savings for only ports that have AES enabled, and PoE priority configured to low.

Prerequisites

Disable AES globally.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **PoePowerSavingEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

Disabling global AES PoE power save mode using EDM

Use the following procedure to disable AES PoE power save mode for the switch.

When enabled, AES PoE power save mode provides the capability to control power consumption savings for only ports that have AES enabled, and PoE priority configured to low.

Prerequisites

Disable AES globally.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **PoePowerSavingEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

Enabling AES efficiency mode using EDM

Use the following procedure to enable AES efficiency mode for the switch.

When enabled, AES efficiency mode enables AES globally and for each port, enables AES PoE power save mode, and configures AES scheduling to predetermined values (on time 18:00 and off time 07:30 daily).

Important:

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.

Prerequisites

Disable AES globally.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **EfficiencyModeEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

Disabling AES efficiency mode using EDM

Use the following procedure to disable AES efficiency mode for the switch.

When enabled, AES efficiency mode enables AES globally and for each port, enables AES PoE power save mode, and configures AES scheduling to predetermined values (on time 18:00 and off time 07:30 daily).

Prerequisites

Disable AES globally.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **EfficiencyModeEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

AES schedule configuration using EDM

Use the information in this section to configure a time interval for the switch to enter lower power states.

Configuring the AES schedule on time using EDM

Use the following procedure to configure the start 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.

Prerequisites

Disable AES globally.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-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, select a radio 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** section.
7. To choose a portion of an hour for the AES schedule on time, type a value in the **ScheduleMinute** section.
8. To configure the selected day, hour, and minutes as the AES schedule on time, select the **activate** radio button in the ScheduleAction section.

   Activate is selected by default.
9. Click **Insert**.

Variable definitions

The following table describes the fields of Insert Energy Saver Schedule screen.

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.

Configuring the AES schedule off time using EDM

Use the following procedure to configure the 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.

Prerequisites

Disable AES globally.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-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 off time, select a radio button in the **ScheduleDay** section.
6. To choose an hour of the day for the AES schedule off time, type a value in the **ScheduleHour** section.
7. To choose a portion of an hour for the AES schedule off time, type a value in the **ScheduleMinute** section.
8. To configure the selected day, hour, and minutes as the AES schedule off time, select the **deactivate** radio button in the ScheduleAction section.

   Activate is selected by default.
9. Click **Insert**.

Modifying an AES schedule on and off time status using EDM

Use the following procedure to change an existing schedule off time to on time or to change an existing schedule on time to off time.

Prerequisites

Disable AES globally.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-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 row, double-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**.

Port-based AES configuration using EDM

Configure port-based AES to enable or disable energy saving for individual ports, or all ports on a switch or stack.

Enabling AES on individual ports using EDM

Use the following procedure to turn on AES for individual ports on a switch or stack.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **ports** tab.
4. Select a **Port**.
5. In the Port row, double-click the cell in the **EnergySaverEnabled** column.
6. Select **true** from the list.
7. Repeat steps 4, 5 and 6 to enable AES for additional ports as required.
8. Click **Apply**.
9. On the toolbar, you can click **Refresh** to update the work area data display.

Variable definitions

The following table describes the fields of Ports tab.

Variable	Value
Port	Indicates the port.
EnergySaverEnabled	Indicates whether the Avaya Energy Saver feature is enabled for the port.

Disabling AES on individual ports using EDM

Use the following procedure to turn off AES for individual ports on a switch or stack.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **ports** tab.
4. Select a **Port**.
5. In the Port row, double-click the cell in the **EnergySaverEnabled** column.
6. Select **false** from the list.
7. Repeat steps 4, 5 and 6 to disable AES for additional ports as required.
8. Click **Apply**.
9. On the toolbar, you can click **Refresh** to update the work area data display.

Viewing AES information using EDM

Use the following procedure to display energy saving information for an individual switch or switches in a stack.

Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-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

Use the data in this table to help you understand the displayed AES information.

Variable	Value
Total	Indicates the total power saving values for all switches in a stack.
UnitIndex	Indicates the unit number of the switch.

Variable	Value
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 8: Configuration reference

The sections in this chapter provide information on the factory default configuration.

Factory default configuration

When you initially access a newly installed switch or you reset a switch to factory defaults, the switch is in a factory default configuration. This factory default configuration is the base configuration from which you build the switch configuration.

Table 93: Factory default configuration settings on page 357 outlines the factory default configuration settings present in a switch in a factory default state.

Table 93: Factory default configuration settings

Setting	Factory default configuration value
Unit Select switch	non-Base
Unit	1
BootP Request Mode	BootP When Needed
In-Band Stack IP Address	0.0.0.0 (no IP address assigned)
In-Band Switch IP Address	0.0.0.0 (no IP address assigned)
In-Band Subnet Mask	0.0.0.0 (no subnet mask assigned)
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

Setting	Factory default configuration value
MAC Address Security	Disabled
MAC Address Security SNMP-Locked	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
Clear by Ports	NONE
Learn by Ports	NONE
Trunk	blank field
Security	Disabled
Port List	blank field
Allowed Source	- (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
Filter Untagged Frames	No
Filter Unregistered Frames	Yes
Port Name	Unit 1, Port 1
PVID	1
Port Priority	0
Tagging	Untag All
AutoPVID	Enabled
Status	Enabled (for all ports)
Linktrap	On
Autonegotiation	Enabled (for all ports)

Setting	Factory default configuration value
Speed/Duplex	(Refer to Autonegotiation)
Trunk	1–8(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 #8
Traffic Type	Rx and Tx
Monitoring Mode	Disabled
Rate Limit Packet Type	Both
Limit	None
Snooping	Disabled
Proxy	Disabled
Robust Value	2
Query Time	125 seconds
Set Router Ports	Version 1
Static Router Ports	- (for all ports)
Console Port Speed	9600 baud
Console Switch Password	None
Telnet/Web Stack Password	None
Console Read-Only Switch Password	user
Console Read/Write Switch Password	Passwords are user/secure for non-SSH SW images and userpasswd/securepasswd for SSH SW images.
Console Read-Only Stack Password	user
Console Read/Write Stack Password	secure
Radius password/server	secret
New Unit Number	Current stack order
Group	1
Bridge Priority	8000
Bridge Hello Time	2 seconds

Setting	Factory default configuration value
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
TELNET Access/SNMP/Web	By default, SNMP access is disabled in the SSH image and enabled in the non-SSH image. Telnet and Web are 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)	Entry 51: ::/0 Entry 52: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 Entry 53: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 ………………………………………………………………. Entry 100: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
	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)
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

Setting	Factory default configuration value
Retrieve Configuration Image from Server	No
ASCII Configuration Filename	Zero-length string
Retrieve Configuration file from Server	No
Auto Configuration on Reset	Disabled
EAPOL Security Configuration	Disabled
High Speed Flow Control Configuration	
VLAN Configuration Control	Strict
Agent Auto Unit Replacement	Enabled