



# **Configuration — System Avaya Ethernet Routing Switch 5000 Series**

6.2  
NN47200-500, 06.03  
March 2012

## 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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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(s) 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 this product. 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://www.avaya.com/support>. Please note that if you acquired the product 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

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

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is

protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

## Third-party components

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://www.avaya.com/support/Copyright/>.

## Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

## Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

## 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://www.avaya.com/support>

# Contents

<b>Chapter 1: New in this release</b> .....	11
Features.....	11
Other changes.....	14
<b>Chapter 2: Introduction</b> .....	17
ACL command modes.....	17
<b>Chapter 3: System configuration fundamentals</b> .....	21
Feature licensing.....	21
User access limitations.....	22
Customizing CLI banner.....	22
TFTP server.....	23
Configuration downloads to a switch.....	23
Multiple switch configuration management.....	25
Secure Shell File Transfer Protocol (SFTP over SSH).....	25
Stacking fundamentals.....	25
Avaya Energy Saver.....	31
Boot agent image.....	32
Supported BootP modes.....	36
IPv6 management.....	36
Dynamic Host Configuration Protocol.....	46
Simple Network Time Protocol.....	47
Ping enhancement.....	47
Auto-MDI X.....	48
Auto-polarity.....	48
Autosensing and autonegotiation.....	48
Quick install.....	54
Set IP parameters using IP.CFG file on a USB memory device.....	54
<b>Chapter 4: Power over Ethernet fundamentals</b> .....	57
PoE overview.....	58
Power source.....	59
Stacking.....	59
Power pairs.....	59
Diagnosing and correcting PoE problems.....	60
Power management.....	62
<b>Chapter 5: LLDP fundamentals</b> .....	65
Link Layer Discover Protocol (IEEE 802.1ab) Overview.....	65
LLDP operational modes.....	66
Connectivity and management information.....	66
802.1AB MED network policies.....	70
Avaya Automatic QoS enhancement for LLDP-MED.....	70
<b>Chapter 6: System configuration with CLI</b> .....	71
General switch administration with CLI.....	71
Stack manager.....	73
Multiple switch configurations.....	74
New Unit Quick Configuration.....	76

IP blocking.....	78
Assigning and clearing IP addresses.....	79
Assigning and clearing IP addresses for specific units.....	84
Displaying interfaces.....	85
Setting port speed.....	86
Testing cables with the Time Domain Reflectometer.....	89
Enabling Autotopology.....	90
Enabling flow control.....	92
Enabling rate-limiting.....	94
Using Simple Network Time Protocol.....	96
Real time clock configuration.....	102
Custom Autonegotiation Advertisements.....	104
Connecting to Another Switch.....	106
Domain Name Server (DNS) Configuration.....	107
Auto Unit Replacement using the ACLI.....	110
Viewing Auto Unit Replacement using the ACLI.....	111
Enabling Auto Unit Replacement using the ACLI.....	112
Disabling AUR using the ACLI.....	112
Restoring the default setting for AUR using the ACLI.....	112
Configuring AUR operation settings using the ACLI.....	112
Avaya Energy Saver configuration using the ACLI.....	113
Configuring global AES using the ACLI.....	114
Configuring port-based AES using the ACLI.....	116
Activating or deactivating AES manually using the ACLI.....	116
Configuring AES scheduling using the ACLI.....	117
Disabling AES scheduling using the ACLI.....	118
Configuring AES scheduling to default using the ACLI.....	119
Viewing AES scheduling using the ACLI.....	120
Viewing AES savings using the ACLI.....	120
Viewing the global AES configuration using ACLI.....	120
Viewing port-based AES configuration using the ACLI.....	121
Changing switch software in the ACLI.....	122
Configuration files in ACLI.....	124
Displaying the current configuration.....	124
Storing the current configuration.....	125
Restoring a system configuration.....	127
Saving the current configuration.....	128
Automatically downloading a configuration file with ACLI.....	129
Terminal setup.....	130
Setting the default management interface.....	131
Setting Telnet access.....	131
telnet-access command.....	132
no telnet-access command.....	133
default telnet-access command.....	134
Setting boot parameters.....	134
Defaulting to BootP-when-needed.....	135
Configuring with the command line interface.....	135

ip bootp server command.....	135
no ip bootp server command.....	136
default ip bootp server command.....	136
shutdown command.....	136
reload command.....	137
ACLI Help.....	138
Clearing the default TFTP server with ACLI.....	138
Configuring a default TFTP server with ACLI.....	139
Displaying the default TFTP server with ACLI.....	139
Secure Transfer File Protocol configuration.....	139
Uploading a config file to an SFTP server.....	140
Downloading a config file to an SFTP server.....	141
Host keys.....	142
Enabling DSA authentication.....	143
Disabling DSA authentication.....	143
Enabling Password authentication.....	143
Disabling Password authentication.....	144
Setting the Transmission Control Protocol port.....	144
Setting timeout.....	145
Viewing SFTP.....	145
Configuring daylight savings time with ACLI.....	146
Configuring default clock source with ACLI.....	147
Configuring local time zone with ACLI.....	147
Configuring Dual Agent with ACLI.....	148
Enhanced download command.....	148
Set the next boot Image.....	150
Show agent images.....	150
Configuring IPv6 with ACLI.....	151
Enabling IPv6 interface on the management VLAN.....	152
Configuring IPv6 interface on the management VLAN.....	152
Displaying the IPv6 interface information.....	153
Displaying IPv6 interface addresses.....	153
Configuring an IPv6 address for a switch or stack.....	154
Displaying the IPv6 address for a switch or stack.....	155
Configuring IPv6 management interface.....	156
Disabling IPv6 globally.....	157
Returning IPv6 to default settings.....	157
Configuring IPv6 global properties.....	158
Displaying the global IPv6 configuration.....	158
Configuring an IPv6 default gateway for the switch or stack.....	159
Displaying the IPv6 default gateway.....	159
Configuring the IPv6 neighbor cache.....	160
Displaying the IPv6 neighbor information.....	160
Displaying IPv6 interface ICMP statistics.....	161
Displaying IPv6 interface statistics.....	162
Displaying IPv6 TCP statistics.....	162
Displaying IPv6 TCP connections.....	163

Displaying IPv6 TCP listeners.....	163
Displaying IPv6 UDP statistics and endpoints.....	163
Configuring LLDP with ACLI.....	164
lldp command.....	165
lldp port command.....	165
lldp tx-tlv command.....	166
lldp tx-tlv dot1 command.....	167
lldp tx-tlv dot3 command.....	167
lldp tx-tlv med command.....	168
lldp location-identification coordinate-base command.....	169
lldp location-identification civic-address command.....	170
lldp location-identification ecs-elin command.....	171
default lldp command.....	172
default lldp port command.....	172
default lldp tx-tlv command.....	173
default lldp tx-tlv dot1 command.....	174
default lldp tx-tlv dot3 command.....	174
default lldp tx-tlv med command.....	175
no lldp port command.....	176
no lldp tx-tlv command.....	176
no lldp tx-tlv dot1 command.....	176
no lldp tx-tlv dot3 command.....	177
no lldp tx-tlv med command.....	177
show lldp command.....	177
show lldp port command.....	179
Configuring LLDP MED policies for switch ports.....	180
Setting lldp med-network-policies to the default values.....	181
Disabling LLDP MED policies for switch ports.....	181
Viewing lldp med-network-policies.....	182
Configuring LLDP.....	183
Configuring PoE detection method with ACLI.....	190
Configuring PoE with ACLI.....	190
Set port power enable or disable.....	190
Set port power priority.....	191
Set power limit for channels.....	191
Set traps control.....	192
Show main power status.....	192
Set power usage threshold.....	192
Setting PoE detection method.....	193
Show port power status.....	193
Show port power measurement.....	194
Customizing ACLI banner with ACLI.....	194
show banner command.....	194
banner command.....	195
no banner command.....	195
Displaying complete GBIC information.....	196
Displaying hardware information.....	196

Configuring AUR with ACLI .....	196
show stack auto-unit-replacement command.....	197
stack auto-unit-replacement enable command.....	198
no stack auto-unit-replacement enable command.....	198
default stack auto-unit-replacement enable command.....	198
stack auto-unit-replacement config save enable.....	198
stack auto-unit-replacement config save disable.....	198
stack auto-unit-replacement config restore unit.....	199
stack auto-unit-replacement config save unit.....	199
Agent Auto Unit Replacement (AAUR).....	199
stack auto-unit-replacement-image enable command.....	199
no stack auto-unit-replacement-image-enable command.....	200
default stack auto-unit-replacement-image enable command.....	200
show stack auto-unit-replacement-image command.....	200
Enabling Autosave.....	201
Disabling Autosave.....	201
Setting Stack Forced Mode.....	202
Configuring stack forced-mode.....	202
Enabling feature license files.....	203
Setting user access limitations.....	204
Setting the read-only and read-write passwords.....	204
Enabling and disabling passwords.....	205
Configuring RADIUS authentication.....	206
Related RADIUS Commands.....	207
Configuring serial console port and USB host port.....	207
Restoring factory default.....	211
<b>Chapter 7: System configuration with Enterprise Device Manager.....</b>	<b>213</b>
Configuring Quick Start using EDM.....	214
Configuring remote access using EDM.....	214
Configuring the IPv4 remote access list using EDM.....	215
Configuring the IPv6 remote access list using EDM.....	216
Viewing PoE ports with Enterprise Device Manager.....	217
General Switch Administration with Enterprise Device Manager.....	218
Displaying the Unit dialog box.....	218
Displaying the Chassis dialog box.....	221
Displaying the Switch/Stack dialog box.....	226
Displaying the Ports dialog box.....	230
Displaying the Environment dialog box.....	242
Avaya Energy Saver configuration using Enterprise Device Manager.....	244
Global AES configuration.....	244
AES schedule configuration.....	248
Port-based AES configuration.....	250
Viewing AES information using EDM.....	252
Bridge configuration using Enterprise Device Manager.....	253
Displaying bridge information.....	253
Displaying the Transparent tab.....	254
Displaying the Forwarding tab.....	255

File System configuration using Enterprise Device Manager.....	256
Config/Image/Diag file tab.....	256
ASCII file tab.....	260
Configuring the license file.....	263
File configuration.....	264
Displaying Boot Image information.....	266
Displaying the Help File Path tab.....	267
ADAC Configuration using Enterprise Device Manager.....	267
Displaying the ADAC tab.....	267
Displaying the ADAC MAC Ranges tab.....	268
Displaying the ADAC Ports tab.....	269
Topology configuration using Enterprise Device Manager.....	270
Viewing topology information.....	270
Viewing topology table information.....	271
System Log configuration using Enterprise Device Manager.....	272
Viewing system log settings.....	272
Viewing remote system log properties.....	273
Viewing system logs.....	274
LLDP configuration using Enterprise Device Manager.....	275
Configuring LLDP transmit properties.....	275
Configuring LLDP ports.....	279
TX Stats.....	281
RX Stats.....	282
Viewing LLDP local system properties.....	284
Viewing LLDP local port properties.....	286
Viewing LLDP management properties.....	287
Viewing LLDP remote management properties.....	288
Viewing unknown TLVs received.....	289
Viewing LLDP organizationally-specific properties.....	290
LLDP Port dot1 configuration using Enterprise Device Manager.....	291
Viewing LLDP VLAN ID properties.....	291
Viewing LLDP protocol VLAN properties.....	292
Viewing LLDP VLAN Name properties.....	293
Viewing LLDP protocol properties.....	293
Viewing LLDP VLAN ID properties.....	294
Viewing LLDP Neighbor Protocol VLAN properties.....	295
Viewing LLDP VLAN Name properties.....	296
Viewing LLDP Neighbor Protocol properties.....	296
LLDP Port dot3 configuration using Enterprise Device Manager.....	297
Viewing LLDP auto-negotiation properties.....	298
Viewing LLDP PoE properties.....	298
Viewing LLDP link aggregation properties.....	299
Viewing LLDP maximum frame size properties.....	300
Viewing LLDP neighbor auto-negotiation properties.....	301
Viewing LLDP neighbor PoE properties.....	301
Viewing LLDP neighbor link aggregation properties.....	303
Viewing LLDP neighbor maximum frame size properties.....	303



LLDP Port MED configuration using Enterprise Device Manager.....	304
Viewing local policy properties.....	305
Local Location.....	306
Viewing LLDP local PoE PSE properties.....	309
Viewing LLDP neighbor capabilities properties.....	310
Viewing LLDP neighbor policy properties.....	311
Neighbor Location.....	312
Viewing LLDP neighbor PoE properties.....	314
Viewing LLDP neighbor PoE PSE properties.....	315
Viewing LLDP neighbor PoE PD properties.....	316
Viewing LLDP neighbor inventory properties.....	317
LLDP MED policy management using Enterprises Device Manager.....	318
Viewing LLDP MED policies.....	319
Creating LLDP MED policies.....	320
Editing LLDP MED policies.....	321
Deleting LLDP MED policies.....	323
SNTP configuration using Enterprise Device Manager.....	323
Displaying the Simple Network Time Protocol tab.....	323
Setting the local time zone.....	324
Configuring daylight savings time.....	325
Displaying the Summer Time Recurring tab.....	326
Power over Ethernet configuration with Enterprise Device Manager.....	327
Viewing global PoE properties for a unit.....	328
Viewing PoE properties for a port.....	329
IPv6 configuration using Enterprise Device Manager.....	330
Configuring IPv6 global properties.....	330
Displaying the ICMP Stats tab.....	331
Displaying the ICMP Msg Stats tab.....	332
Viewing SFP GBIC ports.....	332
<b>Chapter 8: Configuration reference.....</b>	<b>333</b>
Factory default configuration.....	333
<b>Index.....</b>	<b>339</b>



# Chapter 1: New in this release

The following sections detail what's new in Avaya Ethernet Routing Switch 5000 Series software release 6.2.

- [Features](#) on page 11
- [Other changes](#) on page 14

---

## Features

See the following sections for feature changes:

- [Software Licensing enhancements](#) on page 11
- [Running configuration ACLI display command enhancements](#) on page 12
- [Avaya Energy Saver](#) on page 12
- [Route scaling](#) on page 12
- [Secure Shell File Transfer Protocol \(SFTP over SSH\)](#) on page 12
- [SFP support](#) on page 13
- [802.1AB \(LLDP\) MED Network Policy](#) on page 14

---

## Software Licensing enhancements

Software Licensing is a mechanism that allows you to use designated features, according to the license level that you purchase. In Release 6.2 the licensing process is simplified so that if you purchase a license, it remains valid when you upgrade to a version of software that includes additional features included in the license level—that is, you do not have to regenerate the license file, remove the old license from your switches and reload a new license file. Licensing is further simplified for a stack scenario. Automatic Unit Replacement has been updated to enable automatic update of a license for any replacement stack unit, including the Base Unit. For more information, see:

- [Auto Unit Replacement \(AUR\)](#) on page 28
- [Auto Unit Replacement using the ACLI](#) on page 110
- [Configuring AUR](#) on page 225

---

## Running configuration ACLI display command enhancements

The `show running-config` ACLI command enhancements change the operation of the `show running-configuration` command. By default, `show running-configuration` displays only parameters that differ from the default configuration. You can use the verbose qualifier to display the entire ASCII configuration for the switch or stack. You can also use the module qualifier in the command to display the ASCII configuration for a specific feature. For more information, see [Displaying the current configuration](#) on page 124

The operation of the `copy running-config tftp` ACLI command is modified. By default, `copy running-config tftp` copies the complete contents of the running configuration file to a specified file on the TFTP server. With Release 6.2, you can use the module qualifier in the command to display the ASCII configuration for a specific feature, or you can use the verbose qualifier to copy the entire ASCII configuration for the switch or stack. For more information, see [Storing the current configuration](#) on page 125

---

## Avaya Energy Saver

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

- [Avaya Energy Saver](#) on page 31
- [Avaya Energy Saver configuration using the ACLI](#) on page 113
- [Avaya Energy Saver configuration using Enterprise Device Manager](#) on page 244

---

## Route scaling

Up to 4000 routes, a doubling of routes available in the previous release, are available for the Ethernet Routing Switch 5600 Series products.

---

## Secure Shell File Transfer Protocol (SFTP over SSH)

For enhanced network security, Secure FTP for secure file transfer over an SSH session is available in this release. For more information, see

- [Secure Shell File Transfer Protocol \(SFTP over SSH\)](#) on page 25
- [Secure Transfer File Protocol configuration](#) on page 139

---

## SFP support

Release 6.2 supports the following additional SFPs:

- AA1419050-E6
- AA1419051-E6
- AA1419051-E6
- AA1419053-E6
- AA1419054-E6
- AA1419055-E6
- AA1419056-E6
- AA1419057-E6
- AA1419058-E6
- AA1419059-E6
- AA1419059-E6
- AA1419060-E6
- AA1419061-E6
- AA1419062-E6
- AA1419063-E6
- AA1419064-E6
- AA1419065-E6
- AA1419066-E6
- AA1419067-E6
- AA1419068-E6
- AA1419071-E6
- AA1403007-E6
- AA1419074-E6
- AA1419075-E6
- AA1419076-E6
- AA1419077-E6

For more information, see *Avaya Ethernet Routing Switch 5000 Series — Installation SFPs and XFPs*, (NN47200-302).

---

## 802.1AB (LLDP) MED Network Policy

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.

When Automatic QoS is enabled, MED network policy is changed from the user defined DSCP value to DSCP 47 (0x2F) .

You can configure MED network policies on a switch port that has ADAC enabled. The network policies have priority over the ADAC configuration on the port. For more information, see:

- [802.1AB MED network policies](#) on page 70
- [Configuring LLDP MED policies for switch ports](#) on page 180
- [Setting lldp med-network-policies to the default values](#) on page 181
- [Disabling LLDP MED policies for switch ports](#) on page 181
- [Viewing lldp med-network-policies](#) on page 182
- [LLDP MED policy management using Enterprises Device Manager](#) on page 318

---

## Other changes

See the following sections for information about changes that are not feature-related:

- [Enterprise Device Manager](#) on page 14
- [Multiple Port Configuration](#) on page 14

---

## Enterprise Device Manager

Enterprise Device Manager (EDM) replaces both the Java-based Device Manager and Web-based management user interfaces. EDM is an embedded element management and configuration application for Ethernet Routing Switch 5000 Series switches. EDM provides a Web-based graphical user interface through a standard web browser for the convenience of full configuration and management on the switch, and retains the look and feel of Device Manager. For more information, see [System configuration with Enterprise Device Manager](#) on page 213.

## Multiple Port Configuration

Among the many functions available in EDM, you can configure port-specific features for a single port, a group of ports, or all ports. Multiple Port Configuration appears as a pane in the

work area wherever this function is available. By default the pane appears and you can close and open it with a click of the task bar. For more information about EDM, see *Ethernet Routing Switch 5000 Series Fundamentals*, (NN47200-104).

New in this release



# Chapter 2: Introduction

This document provides the information and procedures required to configure the software for the Avaya Ethernet Routing Switch 5000 Series.

Unless otherwise indicated, this information applies to:

- Avaya Ethernet Routing Switch 5510-24T
- Avaya Ethernet Routing Switch 5510-48T
- Avaya Ethernet Routing Switch 5520-24T-PWR
- Avaya Ethernet Routing Switch 5520-48T-PWR
- Avaya Ethernet Routing Switch 5530-24TFD
- Avaya Ethernet Routing Switch 5698-TFD
- Avaya Ethernet Routing Switch 5698-TFD-PWR
- Avaya Ethernet Routing Switch 5650-TD
- Avaya Ethernet Routing Switch 5650-TD-PWR
- Avaya Ethernet Routing Switch 5632-FD

The term "Ethernet Routing Switch 5000 Series" is used in this document to describe the features common to the switches mentioned above.

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

The Avaya Ethernet Routing Switch 5000 Series switches operate in the Stand-alone Mode and Stacking Mode in this product release. A switch can be in Stand-alone Mode or in Stacking Mode, not both.

---

## ACL command modes

ACL provides the following command modes:

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

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

If no password is set, you can enter ACL 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.

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC 5530-24TFD>	No entrance command, default mode	exit or logout
Privileged EXEC 5530-24TFD#	enable	exit or logout
Global Configuration 5530-24TFD(config)#	configure	mode, enter: end or exit To exit ACLI completely, enter: logout
Interface Configuration 5530-24TFD(config-if)# interface vlan	From Global Configuration mode: To configure a port, enter: interface fastethernet <port number> To configure a VLAN, enter: interface fastethernet <vlan number>	To return to Global Configuration mode, enter: Exit To return to Privileged EXEC mode, enter: end To exit ACLI completely, enter: logout
Router Configuration 5530-24TFD(config-if)#	From Global Configuration mode: To configure OSPF, enter: router ospf To configure RIP, enter: router rip To configure VRRP, enter: router vrrp	To return to Global Configuration mode, enter: Exit To return to Privileged EXEC mode, enter: end To exit ACLI completely, enter: logout

See *Avaya Ethernet Routing Switch 5000 Series Fundamentals* (NN47200-104) for more information about ACLI command modes.

---

## Navigation

- [System configuration fundamentals](#) on page 21
- [Power over Ethernet fundamentals](#) on page 57
- [LLDP fundamentals](#) on page 65
- [System configuration with ACLI](#) on page 71
- [System configuration with Enterprise Device Manager](#) on page 213
- [Configuration reference](#) on page 333



# Chapter 3: System configuration fundamentals

The following sections contain system configuration fundamentals for the Avaya Ethernet Routing Switch 5000 Series.

---

## Feature licensing

An Advanced License or a Trial license is required to enable certain features. These software licenses support the following six features:

- Split Multi-Link Trunking (SMLT)
- Open Shortest Path First (OSPF)
- Virtual Router Redundancy Protocol (VRRP)
- Equal Cost Multi Path (ECMP)
- PIM-SM
- IPv6 Forwarding

For more information about licenses, see *Avaya Ethernet Switch 5000 Fundamentals* (NN47200-104).

---

## Trial license

Beginning with release 6.0, the switch offers a Trial License which enables OSPF, ECMP, VRRP, and SMLT, or any combination thereof for a period of 30 days. At the end of the 30 day trial period, the features will be disabled, with the exception of SMLT.

For more information about licenses, see *Avaya Ethernet Switch 5000 Fundamentals* (NN47200-104).

---

## User access limitations

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

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

**\* Note:**

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

---

## Customizing ACLI banner

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

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 with ACLI, refer to the following procedures:

- [show banner command](#) on page 194
- [banner command](#) on page 195
- [no banner command](#) on page 195

To customize ACLI banner with Enterprise Device Manager, refer to the following procedures:

- [Displaying the Banner tab](#) on page 223
- [Displaying the Custom Banner tab](#) on page 224

---

## TFTP server

Many of the processes in the switch can make use of a Trivial File Transfer Protocol (TFTP) server. The following sections detail how to set a default TFTP server for the switch and to clear these defaults through the command line interface:

- [Configuring a default TFTP server with ACLI](#) on page 139
- [Displaying the default TFTP server with ACLI](#) on page 139
- [Clearing the default TFTP server with ACLI](#) on page 138

---

## Configuration downloads to a switch

The following sections provide information about configuration downloads.

### Navigation:

- [Updating switch software](#) on page 23
- [LED activity during software download](#) on page 24
- [Unit quick configuration feature](#) on page 24
- [ASCII configuration file](#) on page 24

---

## Updating switch software

Updating switch software is a necessary part of switch configuration and maintenance. Updating the version of software running on the switch can be accomplished through ACLI.

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

- The switch has been given a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is present on the network that is accessible by the switch and that has the desired software version loaded.
- If you change the switch software on an Avaya Ethernet Routing Switch 5530-24TFD or 5600 series with software stored on a USB Mass Storage Device, ensure that the Mass Storage Device has the desired software version loaded on it and is inserted into the front panel USB port.
- If you use ACLI, ensure that ACLI is in Privileged EXEC mode.

For details on updating switch software, refer to the following sections

- [Changing switch software in the ACLI](#) on page 122
- [Config/Image/Diag file tab](#) on page 256

---

## LED activity during software download

During the software download process, the port LEDs light one after another in a chasing pattern except for ports 11, 12, 23, and 24 on an Avaya Ethernet Routing Switch 5510-24T and ports 35, 36, 47, and 48 on an Avaya Ethernet Routing Switch 5510-48T.

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.

---

## Unit quick configuration feature

You can use the quick configuration commands to automatically integrate a new unit into a stack. See [New Unit Quick Configuration](#) on page 76 for more information and the commands.

---

## ASCII configuration file

With the Avaya Ethernet Routing Switch 5500 Series you can download a user-editable ASCII configuration file from a TFTP server.

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.

See [Retrieving an ASCII configuration file](#) on page 262 for more information and ACLI commands.



---

## Multiple switch configuration management

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

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

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

- [show nvram block command](#) on page 75
- [copy config nvram block command](#) on page 75
- [copy nvram config block command](#) on page 75

---

## Secure Shell File Transfer Protocol (SFTP over SSH)

With this feature, you can securely transfer a binary configuration file from a switch or stack to an SFTP server or from an SFTP server to the switch or stack using the SFTP protocol with SSH version 2.

Release 6.2 supports the following SFTP features:

- a binary configuration file upload to an SFTP server
- a binary configuration file download from a SFTP the server
- DSA-key authentication
- password authentication
- host key generation
- 1024-bit DSA-key use for authentication

---

## Stacking fundamentals

The following sections provide information on stacking fundamentals.

### Navigation:

- [Stacking capabilities](#) on page 26
- [Stack monitor](#) on page 27
- [Agent Auto Unit Replacement \(AAUR\)](#) on page 28
- [Auto Unit Replacement \(AUR\)](#) on page 28
- [Stack Forced Mode](#) on page 30
- [IP blocking](#) on page 31
- [Avaya Energy Saver](#) on page 31

---

## Stacking capabilities

You can use the Avaya Ethernet Routing Switch 5000 Series switches in either of the following configurations:

- stand-alone
- stack

The Avaya Ethernet Routing Switch 5000 Series switches have a built-in cascade port to stack up to eight units.

A stack can consist of any combination of Avaya Ethernet Routing Switch 5000 Series switches.

### Important:

All units in the stack must use the same software version.

To set up a stack, perform the following procedure.

### Procedure steps

1. Power down all switches.
2. Set the Unit Select switch in the back of the non base units to the off position.
3. Set the Unit Select switch in the back of the base unit to base position.
4. Ensure all the cascade cables are properly connected and screwed into the unit.
5. Power up the stack.

### Important:

In a hybrid stack of Avaya Ethernet Routing Switch 5000 Series, you must set an Avaya Ethernet Routing Switch 5600 Series switch type as the base unit.

---

## Stack monitor

The Avaya Ethernet Routing Switch 5000 series stacks support the following two modes of operation:

- Pure
- Hybrid

You can create a pure stack with up to eight Avaya Ethernet Routing Switch 5500 Series switches or eight Avaya Ethernet Routing Switch 5600 Series switches.

You can create a hybrid or mixed stack of up to eight switches that is a combination of Avaya Ethernet Routing Switch 5500 Series switches and Avaya Ethernet Routing Switch 5600 Series switches.

### Important:

In a hybrid stack of Avaya Ethernet Routing Switch 5000 Series, you must set an Avaya Ethernet Routing Switch 5600 Series switch type as the base unit.

Stack manager is responsible for the following functions that form and maintain a stack.

- Base unit selection.
- Unit discovery.
- Unit number assignment.
- Database exchange.
- Join stack handling.
- Programming the hardware for the stack to function as a system.

Stack manager also handles link events from the Hello module when a unit is added or removed from the stack. Based on the event, the stack manager again runs through the state machine to discover the newly added unit or change the stack configuration. Stack manager supports following stack configurations:

- Ring topology: All the units are connected as a ring.
- Upstream: All the non-base units are upstream to the base unit.
- Downstream: All the non-base units are downstream to the base unit.
- Up Down: Non base units are both upstream and downstream of the base unit.

Stack manager supports a maximum of eight switches in a pure or hybrid stack. Although the design does not restrict the number of ports in a stack, Avaya recommends that the number does not exceed 400 ports.

To create a hybrid stack, you must first set the mode parameter on the Avaya Ethernet Routing Switch 5600 Series switches to hybrid mode. Avaya Ethernet Routing Switch 5500 Series switches do not have a mode parameter.

See [Stack manager](#) on page 73 for more information about the stack manager and the procedure and CLI commands to set the stack manager.

---

## Agent Auto Unit Replacement (AAUR)

Software Release 4.2 and later supports Agent Auto Unit Replacement (AAUR), an enhancement to Auto Unit Replacement.

Enabled by default, AAUR inspects non base replacement units joining a stack. If the replacement units do not contain the same software image as the base unit, AAUR downloads the software image from the base unit to the replacement units.

You can use CLI commands to manage and configure AAUR.

### How AAUR works

- When you insert a replacement unit into an AAUR-enabled stack, AAUR compares the switch software image on the replacement unit to the stack software image.
- If the replacement unit software image differs from the stack software image, AAUR downloads the stack software image from the base unit to the replacement unit.
- The system resets the new unit.
- The new unit becomes a member of the stack after reboot.

Once the replacement unit joins the stack, unless you have disabled Auto Unit Replacement (AUR), AUR installs the configuration from the old unit onto the replacement unit if it has the same hardware configuration, and the system resets the replacement unit. Now all units are running the same software version and the configurations are restored. For more information, see [Auto Unit Replacement \(AUR\)](#) on page 28

For more information about AAUR and CLI commands, see [Agent Auto Unit Replacement \(AAUR\)](#) on page 199.

---

## Auto Unit Replacement (AUR)

Enabled by default, Auto Unit Replacement (AUR) restores the configuration of the original unit to the replacement unit when you replace a unit in a stack. The new unit must be the same hardware configuration as the old, including the same number of ports. If you add a new unit with a different hardware configuration, the system uses the configuration of the new unit.

From Release 6.2 and later, Automatic Unit Replacement (AUR) can automatically update a software feature license for any replacement stack unit, including the Base Unit.

You can disable AUR with CLI and the switch retains the AUR state after a reset. Logs messages are available for AUR.

AUR is not compatible with software versions prior to 4.1.

**! Important:**

For Auto Unit Replacement to operate, stack power must be on during the unit replacement because configuration images are retained in the stack DRAM.

AUR does not work on a stack of only two units because, if a unit fails, the remaining unit becomes a standalone switch and AUR does not load the configuration of the failed unit if it is replaced.

**! Important:**

Avaya recommends that the replacement unit runs the same version of diagnostics as the stack base unit.

When AUR is enabled, you can

- manually restore an associated configuration (same unit number) to a non base unit, regardless of the MAC address
- manually configure a non base unit to the base unit regardless of the state of AUR

When AUR is enabled, you cannot

- manually restore configuration for a base unit
- manually save a configuration for a base unit

**! Important:**

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

After you reboot a stack, you can use ACLI command `show stack auto-unit-replacement` from a unit console to determine whether that unit is ready for replacement.

Following is an example of the command output:

```
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
```

**Figure 1: show stack auto-unit replacement**

For information about configuring AUR with ACLI, see [Configuring AUR with ACLI](#) on page 196.

For information about configuring AUR with Enterprise Device Manager, see [Configuring AUR](#) on page 225.

---

## 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.

For instructions to configure stack forced mode with ACLI, see [Setting Stack Forced Mode](#) on page 202.

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 Enterprise Device Manager.

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 will send 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, then 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 Enterprise Device Manager 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.

---

## IP blocking

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

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

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

---

## Avaya Energy Saver

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

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

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

Avaya recommends disabling AES on uplink copper ports since activating or deactivating AES on copper ports will trigger a link down followed rapidly by a link up event. The best solution

is to use fiber ports for uplinks since link status will not change when AES is activated or deactivated.

**! Important:**

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

---

## Boot agent image

The Dual Agent feature provides support for two agents for Ethernet Routing Switch 5500 or 5600 series in stand-alone, pure stack or for a mixed (hybrid) stack configuration. Dual Agent functionality is not supported on Ethernet Routing Switch 5510.

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

An Ethernet Routing Switch 56xx unit has two combo images in the flash. In another word, an Ethernet Routing Switch 5600 unit has two Ethernet Routing Switch 56xx agent images and two Ethernet Routing Switch 55XX agent images in the flash. An Ethernet Routing Switch 55XX unit has two Ethernet Routing Switch 55XX images in the flash.

In a mixed stack with both Ethernet Routing Switch 5500 units and Ethernet Routing Switch 5600 units, an Ethernet Routing Switch 5600 must be the base unit. For a mixed stack to use the Dual Agent feature, the following conditions must be met:

- All Ethernet Routing Switch 5600 units must have the same agent software version.
- All Ethernet Routing Switch 5500 units must have the same agent software version.
- All unit agent software must have the same Interop Software Version Number (ISVN).

Special Case: If an Ethernet Routing Switch 5510 is the base unit, Dual Agent is disabled in the stack.

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

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

---

## Next Boot image and system Boot-up in Dual Agent

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

When an agent image is downloaded to the switch, the unit resets and boots up with the newly downloaded image regardless of the value of the Next Boot image indicator. If an agent image



is downloaded to the switch without a reset of the unit, the newly downloaded image becomes the Next Boot image.

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

## System boot-up for stand-alone

A stand-alone unit boots up with the Next Boot image from the NVRAM.

## System boot-up for stack

The following lists the boot-up sequence:

- All the units in the stack start up with the Next Boot image.
- The stack does the following operations in the stack discovery phase:
  - The Next Boot image in the BU is used as the reference image.
  - If the Next Boot image in the NBU matches with the BU Next Boot image, the NBU continue to boot with the current Next Boot image.
  - If both images in the NBU do not match with the BU Next Boot image, the unit continues to boot with the current Next Boot image.
  - If the Next Boot image in the NBU does not match with the BU Next Boot image, but the other image in the NBU is matched, the matched image is selected as the Next Boot image then the unit is reset.

## Dual Agent and Ethernet Routing Switch 5510

Dual Agent supports an Ethernet Routing Switch 5510 NBU with AAUR.

The following example shows how Dual Agent uses AAUR in a stack that contains Ethernet Routing Switch 5510 NBUs if you toggle the Next Boot image:

- All units in the stack reset with the new Next Boot image except for the Ethernet Routing Switch 5510 NBUs that will reset with only the agent image because they do not have the second image.
- All the units join stack except for the Ethernet Routing Switch 5510 units that now become stand-alone units because the agent image is now different from the one from in the stack.
- The Ethernet Routing Switch 5510 stand-alone units get the new image from the stack through AAUR and join the stack.

The following graphic shows what happens when you toggle the Next Boot image:

```
5650TD (config)#show boot image
```

UNIT	PRIMARY	SECONDARY	ACTIVE
1	6.1.0.141	6.1.0.140	6.1.0.141
2	6.1.0.141	6.1.0.140	6.1.0.141
3	6.1.0.141	6.1.0.140	6.1.0.141

```
5650TD (config)#toggle-next-boot-image
5650TD (config)#show boot image
```

UNIT	PRIMARY	SECONDARY	ACTIVE
1	6.1.0.140	6.1.0.141	6.1.0.141
2	6.1.0.140	6.1.0.141	6.1.0.141
3	6.1.0.140	6.1.0.141	6.1.0.141

```
5650TD (config)#boot
```

**Figure 2: show boot image**

After the restart, the device starts up with version 6.2.0.140. This becomes the active image:

```
5650TD (config)#show boot image
```

UNIT	PRIMARY	SECONDARY	ACTIVE
1	6.1.0.140	6.1.0.141	6.1.0.140
2	6.1.0.140	6.1.0.141	6.1.0.140
3	6.1.0.140	6.1.0.141	6.1.0.140

**Figure 3: show boot image after restart**

---

## Combination image

The Combination (Combo) Agent Image contains the header of the image and two agent images, a 56xx agent image and a 55XX agent image.

---

## Download combination image

Any 55xx software release before release 6.0 does not support the Combo image.

A stand-alone unit or a stack that uses the Ethernet Routing Switch 5000 Series Software Release 6.2 can download a combo image. Release 6.2 is available in two different formats: a file in Combo format version 6.2 and a file in 55xx image format version 6.2.

The 55xx image format in this release is necessary because not all of the current 55xx releases support the Combo image.

## Ethernet Routing Switch 5600 stand-alone

The unit downloads the combo image through the TFTP or USB port then stores the image in a flash device.

## Ethernet Routing Switch 5000 Series mixed stack

The base unit receives the combo image through the TFTP or USB port then transfers the image to the non-base units. The Ethernet Routing Switch 5600 unit non-base units receive the combo image and the Ethernet Routing Switch 5500 non-base units receive the 5500 series image that is extracted from the combo image.

All of the units in the stack store the received image in flash devices.

## Ethernet Routing Switch 5500 stand-alone

The unit extracts the 5500 series image from the combo image through the TFTP or USB port then stores the image in a flash device.

## Ethernet Routing Switch 5000 Series mixed stack

The base unit extracts the 5500 series image through the TFTP or USB port then transfers the image to the non-base units.

All of the units in the stack store the received image in flash devices.

---

## Combo Diagnostic Image

The Combo Diagnostic Image contains the header of the image and two Diagnostic images: a 56xx diagnostic image and a 55xx diagnostic image.

Any 55xx software release before release 6.0 does not support the Combo Diagnostic image.

A stand-alone unit or a stack that uses the Ethernet Routing Switch 5000 Series software release 6.0 can download a combo diagnostic image.

This diagnostic release for the new software release 6.2 is available in two different formats: a file in Combo format and a file in 55xx format. The 55xx image format in this release is necessary because all the current 55xx releases do not support the Combo diagnostic image.

The considerations for downloading a Combo Agent Image also apply to downloading a Combo Diagnostic Image.

---

## Supported BootP modes

The following section describes the supported BootP modes.

### Navigation:

- [BootP mode](#) on page 36

---

## BootP mode

The Avaya Ethernet Routing Switch 5000 Series supports the Bootstrap protocol (BootP).

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

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

The Avaya Ethernet Routing Switch 5000 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 5000 Series BootP requests.

The BootP modes supported by the Avaya Ethernet Routing Switch 5000 Series are:

- BootP or Last Address mode
- BootP When Needed. This is the default mode.
- BootP Always
- BootP Disabled. Disabling BootP also disables DHCP.

---

## IPv6 management

This module provides information about the IPv6 management feature of the Avaya Ethernet Routing Switch 5000 Series switch platforms.

---

## Navigation

- [The IPv6 header](#) on page 38
- [IPv6 addresses](#) on page 38
- [Table 1: IPv6 address format](#) on page 38
- [Interface ID](#) on page 38
- [Address formats](#) on page 39
- [IPv6 extension headers](#) on page 39
- [Comparison of IPv4 and IPv6](#) on page 40
- [ICMPv6](#) on page 41
- [Neighbor discovery](#) on page 41
- [ND messages](#) on page 43
- [Neighbor discovery cache](#) on page 44
- [Router discovery](#) on page 45
- [Path MTU discovery](#) on page 46
- [Router discovery](#) on page 45
- [Router advertisement](#) on page 45
- [Router solicitation](#) on page 45
- [Path MTU discovery](#) on page 46

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 5000 Series switches function as a dual stack network node).

IPv6 routing is supported in the current phase. You can perform IPv6 interface configuration with ACLI or SNMP (Enterprise Device Manager). For more control over IPv6, use ACLI or Enterprise Device Manager.

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 rclpv6.

---

## 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.

The following table shows the IPv6 address format.

**Table 1: IPv6 address format**

Type	Address	Interface ID (or token)
------	---------	-------------------------

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 is the hexadecimal representation of 16 bits in the address. An example is as follows:

FF01:0:0:0:0:0:43

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:d.d.d.d

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

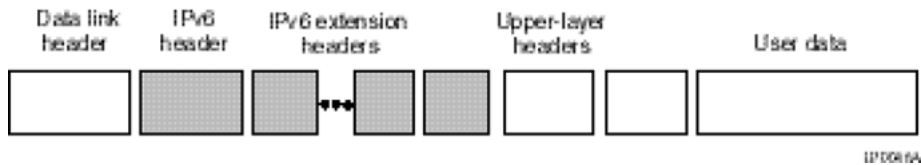
or

::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. The following graphic shows the IPv6 header and extension headers:



**Figure 4: 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.
- The fragmentation extension header uses an IPv6 source to send packets larger than the size specified for the path maximum transmission unit (MTU).
- 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 2: IPv4 and IPv6 differences**

Feature	IPv4	IPv6
<sup>1</sup> Ethernet Routing Switch 5000 Series does not support IPsec. <sup>2</sup> Ethernet Routing Switch 5000 Series does not perform Router discovery or advertise as a router. <sup>3</sup> Ethernet Routing Switch 5000 Series does not implement any form of automatic configuration of IPv6 address in release 6.0.		
Address length	32 bits	128 bits
IPsec support <sup>1</sup>	Optional	Required



Feature	IPv4	IPv6
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
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router discovery <sup>2</sup>	Optional	Required
Uses broadcasts	Yes	No
Configuration <sup>3</sup>	Manual, DHCP	Automatic, DHCP

---

## 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

The following graphic shows the neighbor discovery components:

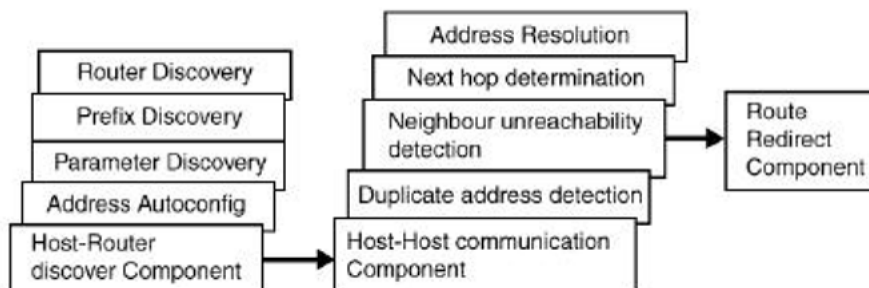


Figure 5: Neighbor discovery components

## ND messages

The following table shows new ICMPv6 message types.

**Table 3: IPv6 and IPv4 neighbor 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 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

IPv4 neighbor function	IPv6 neighbor function	Description
		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.
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 4: 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

State	Description
	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 a Multi-Link Trunking port from a VLAN
- removing a 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 destination. If the packet encounters a link with 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.

---

## Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is defined by the RFC 2131. DHCP allows individual TCP/IP hosts on an IP network to obtain their configuration information from a DHCP server (or servers) that have no exact information about the individual hosts until they request configuration parameters. This reduces the work of system administrators, especially in larger IP networks, by eliminating the need to manually set every IP address. The most significant pieces of information distributed through DHCP are:

- the IP address
- the network mask
- the IP address of the gateway

In many networks, DHCP must coexist with VLANs, and the DHCP client can make its broadcasts only in the trusted VLANs. The DHCP client will run at startup just like the BootP client. The DHCP client restricts its discovery broadcasts to the management VLAN.

The DHCP modes supported by the Avaya Ethernet Routing Switch 5000 Series are:

- DHCP or Last Address mode
- DHCP When Needed.
- DHCP Always
- DHCP Disabled. Disable DHCP by setting BootP Disabled.

The host cannot act as a DHCP relay while the DHCP client is running.

---

## Simple Network Time Protocol

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

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

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

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

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

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

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

---

## 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 information about ACLI ping command, see [ping command](#) on page 106.

## Auto-MDI X

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

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

---

## Auto-polarity

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

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

---

## Autosensing and autonegotiation

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

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

Autosensing is used when the attached device is not capable of autonegotiation or is using a form of autonegotiation that is not compatible with the IEEE 802.3z autonegotiation standard. If it is not possible to sense the duplex mode of the attached device, the Avaya Ethernet Routing Switch 5000 Series reverts to half-duplex mode.

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

### Navigation:

- [Custom Autonegotiation Advertisements](#) on page 49
- [Configuring CANA with ACLI](#) on page 49



- [Viewing current autonegotiation advertisements](#) on page 50
- [Viewing hardware capabilities](#) on page 51
- [Setting default advertisements](#) on page 52
- [Silencing advertisements](#) on page 53

---

## Custom Autonegotiation Advertisements

In the Avaya Ethernet Routing Switch 5000 Series, the Custom Autonegotiation Advertisements (CANA) feature enables you 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 that are supported by the switch and attempt to establish a link at the highest common speed and duplex setting. By using CANA, the port can be configured to advertise only certain speed and duplex settings, thereby allowing links to be established only at these settings, regardless of the highest common supported operating mode.

CANA also enables control over the IEEE802.3x flow control settings advertised by the port, as part of the autonegotiation process. Flow control advertisements can be set to Symmetric, Asymmetric, or Disabled if neither is selected.

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

- If a network can support only 10 Mb/s connection, a port can be configured to advertise only 10 Mb/s capabilities. Devices using autonegotiation to connect to this port connect at 10 Mb/s, even if both devices are capable of higher speeds.
- If a port is configured to advertise only 100 Mb/s full-duplex capability, the link becomes active only if the link partner is also capable of autonegotiating 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, it can be useful to configure a link to autonegotiate at a particular speed or duplex mode.

---

## Configuring CANA with ACLI

Use this procedure to configure CANA.

### Procedure steps

Use the following command from Privileged EXEC mode: `auto-negotiation-advertisements`

Example

To configure port 5 to advertise the operational mode of 10 Mb/s and full duplex, enter the following command line: `auto-negotiation-advertisements port 5 10-full`

The following figure shows sample output for this command.

```
5510-48T(config-if)#auto-negotiation-advertisements port 5 10-full
5510-48T(config-if)#
```

**Figure 6: auto-negotiation-advertisements command sample output**

---

## Viewing current autonegotiation advertisements

Use this procedure to view autonegotiation advertisements for the device.

### Procedure steps

Use the following command from Privileged EXEC mode: `show auto-negotiation-advertisements [port <portlist>]`

The following figure shows an example of the output for the `show auto-negotiation-advertisements` command.

```

5510-48T#show auto-negotiation-advertisements
Port Autonegotiation Advertised Capabilities
-----
 1  10Full 10Half 100Full 100Half 1000Full          Pause
 2  10Full 10Half 100Full 100Half 1000Full          Pause
 3  10Full 10Half 100Full 100Half 1000Full          Pause
 4  10Full 10Half 100Full 100Half 1000Full          Pause
 5  10Full
 6  10Full 10Half 100Full 100Half 1000Full          Pause
 7  10Full 10Half 100Full 100Half 1000Full          Pause
 8  10Full 10Half 100Full 100Half 1000Full          Pause
 9  10Full 10Half 100Full 100Half 1000Full          Pause
10  10Full 10Half 100Full 100Half 1000Full          Pause
11  10Full 10Half 100Full 100Half 1000Full          Pause
12  10Full 10Half 100Full 100Half 1000Full          Pause
13  10Full 10Half 100Full 100Half 1000Full          Pause
14  10Full 10Half 100Full 100Half 1000Full          Pause
15  10Full 10Half 100Full 100Half 1000Full          Pause
16  10Full 10Half 100Full 100Half 1000Full          Pause
17  10Full 10Half 100Full 100Half 1000Full          Pause
18  10Full 10Half 100Full 100Half 1000Full          Pause
19  10Full 10Half 100Full 100Half 1000Full          Pause
20  10Full 10Half 100Full 100Half 1000Full          Pause
----More (q=Quit, space/return=Continue)----

```

**Figure 7: show auto-negotiation-advertisements command sample output**

The following figure shows an example of the output for the `show auto-negotiation-advertisements` command.

```

5510-48T#show auto-negotiation-advertisements port 5
Port Autonegotiation Advertised Capabilities
-----
 5  10Full
5510-48T#

```

**Figure 8: show auto-negotiation-advertisements command sample output**

**\* Note:**

Port 5 has been configured to only advertise an operational mode of 10 Mb/s full duplex

---

## Viewing hardware capabilities

Use this procedure to view the operational capabilities of the device.

## Procedure steps

Use the following command from Privileged EXEC mode: `show auto-negotiation-capabilities [port <portlist>]`

The following figure shows an example of the output for the `show auto-negotiation-capabilities` command.

```
5510-48T#show auto-negotiation-capabilities
Port Autonegotiation Capabilities
-----
 1   10Full 10Half 100Full 100Half 1000Full          Pause
 2   10Full 10Half 100Full 100Half 1000Full          Pause
 3   10Full 10Half 100Full 100Half 1000Full          Pause
 4   10Full 10Half 100Full 100Half 1000Full          Pause
 5   10Full 10Half 100Full 100Half 1000Full          Pause
 6   10Full 10Half 100Full 100Half 1000Full          Pause
 7   10Full 10Half 100Full 100Half 1000Full          Pause
 8   10Full 10Half 100Full 100Half 1000Full          Pause
 9   10Full 10Half 100Full 100Half 1000Full          Pause
10   10Full 10Half 100Full 100Half 1000Full          Pause
11   10Full 10Half 100Full 100Half 1000Full          Pause
12   10Full 10Half 100Full 100Half 1000Full          Pause
13   10Full 10Half 100Full 100Half 1000Full          Pause
14   10Full 10Half 100Full 100Half 1000Full          Pause
15   10Full 10Half 100Full 100Half 1000Full          Pause
16   10Full 10Half 100Full 100Half 1000Full          Pause
17   10Full 10Half 100Full 100Half 1000Full          Pause
18   10Full 10Half 100Full 100Half 1000Full          Pause
19   10Full 10Half 100Full 100Half 1000Full          Pause
20   10Full 10Half 100Full 100Half 1000Full          Pause
----More (q=Quit, space/return=Continue)----
```

**Figure 9: show auto-negotiation-capabilities command sample output**

The following figure shows an example of the output for the `show auto-negotiation-capabilities` command.

```
5510-48T#show auto-negotiation-capabilities port 5
Port Autonegotiation Capabilities
-----
 5   10Full 10Half 100Full 100Half 1000Full          Pause
5510-48T#
```

**Figure 10: show auto-negotiation-capabilities command sample output**

---

## Setting default advertisements

Use this procedure to set default autonegotiation advertisements for the device.

## Procedure steps

Use the following command from Interface Configuration mode: `default auto-negotiation-advertisements [port <portlist>]`

## Example

To set default advertisements for port 5 of the device, enter the following command line:  
`default auto-negotiation-advertisements port 5`

---

## Silencing advertisements

Use this procedure to set a port to not transmit any autonegotiation advertisements.

## Procedure steps

Use the following command from Interface Configuration mode: `no auto-negotiation-advertisements [port <portlist>]`

## Exmale

To silence the autonegotiation advertisements for port 5 of the device, enter the following command line: `no auto-negotiation-advertisements port 5`

The following figure shows an example of the output for the `default auto-negotiation-advertisements` command.

```
5510-48T(config-if)#default auto-negotiation-advertisements port 5
5510-48T(config-if)#
```

Figure 11: default auto-negotiation-advertisements command sample output

The following figure shows an example of the output for the `default auto-negotiation-advertisements` command.

```
5510-48T(config-if)#no auto-negotiation-advertisements port 5
5510-48T(config-if)#
```

Figure 12: no auto-negotiation-advertisements command sample output

---

## Quick install

Quick Install allows users to take first configuration from a file found on a USB device or from a minimal configuration menu.

If the switch does not obtain an IP address using bootp, and, a file named IP.CFG exists on the USB device, then the switch loads the IP.CFG file as its first configuration.

See also [Set IP parameters using IP.CFG file on a USB memory device](#) on page 54.

If the switch cannot find an IP address after the user presses CTRL + Y from long console then it shows a minimal menu. Quick Configuration encompasses multiple menus consolidating them into a single menu for the user to access and make the required initial setup modifications.

The user must enter the following information into the menu:

- IP address
- Sub-net mask
- Default gateway
- Read-only community string
- Read-write community string
- Quick start VLAN

---

## Set IP parameters using IP.CFG file on a USB memory device

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

**\* Note:**

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

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

The following table describes the ip.cfg file parameters:

**Table 5: IP.CFG file parameters**

Parameter	Description
IP <xx.xx.xx.xx>	Specifies the IP address for the switch. Example: 192.168.22.1
Mask <xx.xx.xx.xx>	Specifies the network mask. Example: 255.255.255.0
Gateway <xx.xx.xx.xx>	Specifies the default gateway. Example: 181.30.30.254
SNMPread <string>	Specifies the SNMP read community string. Example: public
SNMPwrite <string>	Specifies the SNMP write community string. Example: private
VLAN <number>	Specifies the management VLAN-ID. Example: VLAN 1
USBdiag <string>	Specifies the filename of the diagnostic image to load from the USB. Example: ers5600/ers5600_6.0.0.10.bin
USBascii <string>	Specifies the filename of the ASCII config file to load from the USB. Example: customer1.cfg
USBagent <string>D NEXTIP, NEXTMask, and NEXTGateway	Specifies the filename of the agent image to load from the USB and specifies IPs for next boot. Example: ers5600/ers5600_6.2.0.0.img

**\* Note:**

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

The ip.cfg file loads information from the ASCII configuration file in order of precedence. For example, if you have an ip.cfg file with the following commands:

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

The stack IP becomes 181.30.30.113 no matter what IP address is in the ip.txt file.

If you have an ip.cfg file with the following commands:

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

The stack IP will be the IP address defined in the ip.txt file.

**\* Note:**

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

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

```
#Any lines starting with a # are comments
#IP <xx.xx.xx.xx> specifies the IP address for the switch
IP 172.16.1.23

#Mask <xx.xx.xx.xx> specifies the network mask Mask 255.255.255.0
#Gateway <xx.xx.xx.xx> specified the default gateway Gateway 172.16.1.1
#SNMPread <string> specified the SNMP read community string SNMPread public
#SNMPwrite <string> specified the SNMP write community string SNMPwrite private
#VLAN <number> specified the management VLAN-ID VLAN 1
#USBdiag <string> specifies the filename of the diagnostic image to load (noreset)
USBdiag ers5600/ers5600_5.1.0.4.bin

#USBagent <string> specifies the filename of the agent image to load (noreset)
USBagent ers5600/ers5600_5.2.0.0.img

#USBascii <string> specifies the filename of the ASCII config file to load
USBascii customer1.cfg

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

### Figure 13: Ip.cfg file example

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

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



# Chapter 4: Power over Ethernet fundamentals

The information in this section provides an overview of Power over Ethernet (PoE). See the *Avaya Ethernet Routing Switch 5000 Series Installation* (NN47200-300) for detailed information about the installation of power supplies and details about PoE.

PoE in Avaya Ethernet Routing Switch 5000 Series switches uses the IEEE 802.3af standard.

PoE is the ability to power network devices over the Ethernet cable. Some such devices include IP Phones, Wireless LAN Access Points, security cameras, access control points, and so on.

The following 5000 Series switches provide PoE:

- Avaya Ethernet Routing Switch 5520-24T-PWR
- Avaya Ethernet Routing Switch 5520-48T-PWR
- Avaya Ethernet Routing Switch 5650-TD-PWR
- Avaya Ethernet Routing Switch 5698-TFD-PWR

The 5000 Series switches support the following PoE features:

- DTE power.
- Powered device (PD) discovery and classification.
- Capacitive detection to support legacy PD devices, including the Avaya and Cisco Legacy IP Phones.
- Port power management and monitoring for each port.
- AC and DC disconnection.
- Detection of load over or under voltage or current.
- PoE status LED for each port.
- Port prioritizing to guarantee DTE power available on high-priority ports
- Port pruning to prevent system failure

You can configure PoE with ACLI or Enterprise Device Manager. See the following sections for details:

- [PoE overview](#) on page 58
- [Power source](#) on page 59
- [Stacking](#) on page 59
- [Power pairs](#) on page 59
- [Diagnosing and correcting PoE problems](#) on page 60

- [Power management](#) on page 62
- [Configuring PoE with ACLI](#) on page 190
- [Viewing PoE ports with Enterprise Device Manager](#) on page 217

---

## PoE overview

The 5000 Series switches are ideal to use with Avaya Business Communication Manager system, IP phones, hubs, and wireless access points. You can use these switches in conjunction with all network devices.

By using the 5000 Series switches, you can plug any IEEE 802.3af-compliant powered device into a front-panel port of a PoE-capable switch and receive power. Data can be passed simultaneously on that port.

The IEEE 802.3af draft standard regulates a maximum of 15.4 watts (W) of power for each port; that is, a power device cannot request more than 15.4 watts (W) of power. As different network devices require different levels of power, the overall available power budget of the 5000 Series switches 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 5000 Series switches automatically detect all IEEE 802.3af-draft-compliant powered devices attached to each front-panel port and immediately sends power to that appliance. The switch also automatically detects how much power each device requires and supplies the required DC voltage at a set current based on the load conditions and current availability. The switch supports both PoE and standard LAN devices.

The power detection function of the 5000 Series switches operate independently of the data link status. Power can be requested by a device that is already operating the link for data, or it can be requested by a device that is not yet operational. That is, the 5000 Series switches provide power to a requesting device even if the data link for that port is disabled. The switch monitors the connection and automatically disconnects power from a port when the device is removed or changed, as well as when a short occurs.

The 5000 Series switches automatically detect those devices that do not require power connections from it, such as laptop computers or other switching devices, and does not send any 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.

**\* Note:**

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

---

## Power source

The Avaya Ethernet Redundant Power Supply 15 is available as an optional external power source for the Avaya Ethernet Routing Switch 5520. Contact your Avaya representative for more information about the Avaya Ethernet Redundant Power Supply Unit 15.

The following are the available options to power the Avaya Ethernet Routing Switch 5520:

- Internal power source only
- External power source only:
  - Avaya Ethernet Redundant Power Supply 15
- Internal power source plus external power source:
  - Avaya Ethernet Redundant Power Supply 15

In a stack configuration, each unit can have its own external power source.

The 5650-TD-PWR and 5698-TFD-PWR switches use modular power supply units. The PoE capability at each 5600 Series switch port depends on the power supply modules that you install. See *Avaya Ethernet Routing Switch 5000 Series Installation* (NN47200-300) for information about the power supplies and PoE.

The PoE capability of each 5650-TD-PWR or 5698-TFD-PWR switch port depends on the power supply modules that you install. See the *Avaya Ethernet Routing Switch 5000 Series Installation* (NN47200-300) for information about the PoE capability at each port as a function of the power supply modules.

---

## Stacking

You can stack the 5000 Series switches up to 8 units high. These stacks also can be configured for redundancy.

---

## Power pairs

The 5000 Series switches support wiring as mentioned in the IEEE 802.3AF draft standard.

The 5000 Series switches supports power to Signal pair only.

See the *Avaya Ethernet Routing Switch 5000 Series Installation* (NN47200-300) for connector pinout tables and wiring specifics.

---

## Diagnosing and correcting PoE problems

This section discusses some common problems that you can encounter while using the PoE features of the 5000 Series switches.

See the *Avaya Ethernet Routing Switch 5000 Series Troubleshooting* (NN47200-700) for detailed troubleshooting information.

### Navigation:

- [Messages](#) on page 60
- [Connecting the PSU](#) on page 60

---

## Messages

The following table describes the error messages displayed by a port that supports PoE.

**Table 6: Error messages displayed by PoE ports**

Error Message	Descriptions
Detecting	The port detects an IP device that is requesting power.
Delivering power	Port delivers the requested power to the IP device.
Disabled	The port power state is disabled.
Invalid PD	The port is detecting a device that is not authorized to request for power.
Deny low priority	Power disabled from the port because of port setting and demands on power budget.
Overload	Power disabled from the port because the port is overloaded.
Test	The port is in testing mode. This was set by using SNMP.
Error	An unspecified error condition has occurred.

---

## Connecting the PSU

Perform this procedure in the order specified to connect the PSU to the Avaya Ethernet Routing Switch 5520.

## Procedure steps

1. Ensure that the DC ON/OFF switch on the back of the Avaya Ethernet Routing Switch 5520 is in the OFF position.
2. Plug the external power source into the DC connector receptacle on the back of the Avaya Ethernet Routing Switch 5520, by using the 2-pin power connector and 10-pin control connector.
3. Attach the ground lug on a cable to a grounding point.
4. Plug the power cord from the Avaya Ethernet RPSU 15 to the wall outlet.
5. Plug the power cord from Avaya Ethernet Routing Switch 5520 into the wall outlet.
6. Turn the DC ON/OFF breaker on the back of the switch to the ON position.

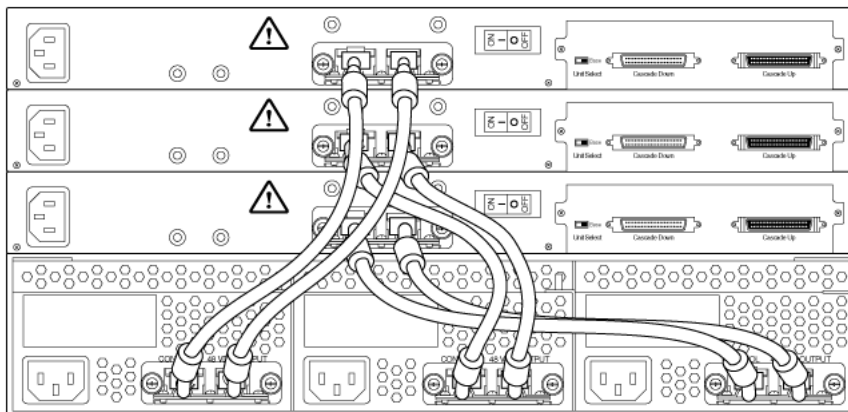
### **⚠ Caution:**

Ensure that the DC ON/OFF breaker is in the OFF position before you connect or disconnect the optional external power source.

The following figure shows 3 Avaya Ethernet RPSU 15s connected to the back of a stack of 3 Avaya Ethernet Routing Switch 5520 switches.

### **\* Note:**

The grounding wire is connected with a screw, and a star washer is provided on the base of the Avaya Ethernet Routing Switch 5520.



553-AAA2984

**Figure 14: External power source connected to back of the Avaya Ethernet Routing Switch 5520**

---

## Power management

The 5000 Series switch uses several device management systems, such as Command Line Interface (CLI), and Enterprise Device Manager, as well as Optivity for network-level management services.

With CLI or Enterprise Device Manager, you can configure the level of power to specific ports, as well as enable or disable power to each port. You can set the maximum power level for each port by increments of 1 W; in the range of 3 to 16 W. The default power level for each port is 16 W.

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. If the power requirements are lower than the switch power budget, the power is returned to the dropped port.

For example, assume the following scenario:

- Ports 1 to 20 are configured as low priority
- Port 21 is configured as high priority
- Ports 1 to 20 are connected to powered devices
- Devices on ports are consuming all the available 5000 Series switch power
- A device is connected to port 21 and requests power

In this scenario, the 5000 Series switch provides power to the device on port 21 because that port is configured as high priority. However, to maintain the power budget, the switch drops one of the ports configured as a lower priority. As all the other ports (1 to 20) are configured with a low priority, the switch drops power to the highest port number. In this case, the switch drops power to port 20 and provides power to port 21. If another port drops power, the switch automatically reinstates power to port 20.

You configure the autodiscovery power process as either IEEE 802.3af compliant or IEEE 802.3af draft compliant and legacy:

- 802.3af -- detection method outlined in IEEE 802.3af draft standard
- legacy -- detection standard in use prior to IEEE 802.3af draft standard

The default value is IEEE 802.3af draft compliant. You can set this parameter for the entire switch; you cannot set the discovery mode for each port.

You can obtain power usage information from the management systems. Statistics do not accumulate. The system automatically disconnects the port from power when it detects overload on any port, and the rest of the ports remain functioning.

**\* Note:**

Ensure that the switch is set for the power detection mode used by the connected powered device. Consult the device documentation for this information.





# Chapter 5: LLDP fundamentals

The information in this section provides an overview of LLDP fundamentals.

## Navigation:

- [Link Layer Discover Protocol \(IEEE 802.1ab\) Overview](#) on page 65
- [LLDP operational modes](#) on page 66
- [Connectivity and management information](#) on page 66
- [802.1AB MED network policies](#) on page 70
- [Avaya Automatic QoS enhancement for LLDP-MED](#) on page 70

---

## Link Layer Discover Protocol (IEEE 802.1ab) Overview

Release 5.0 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.

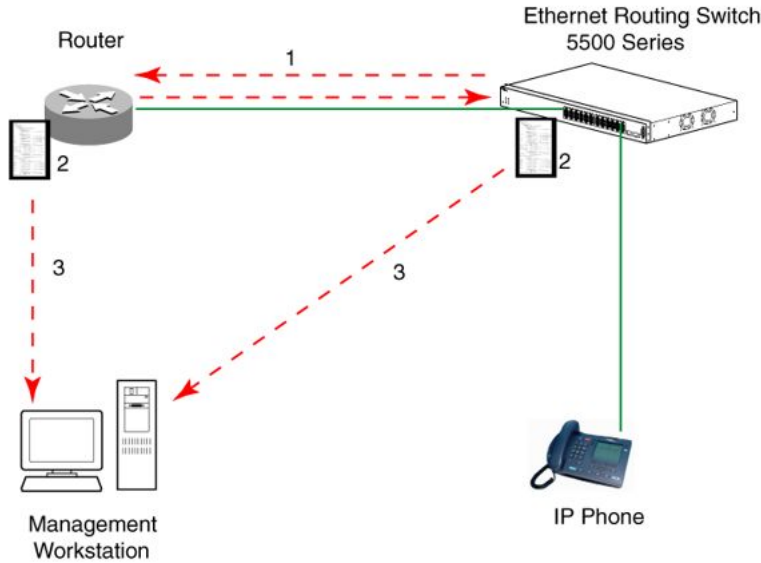
Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with 5000 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).

The following figure shows an example of how LLDP works in a network.



**Figure 15: LLDP: how it works**

1. The Ethernet Routing Switch and LLDP-enabled router advertise chassis and port IDs and system descriptions (if enabled) 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 contained 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.

In addition to the four mandatory TLVs, Release 5.0 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, refer to the following:

- [Management TLVs](#) on page 67
- [IEEE 802.1 organizationally-specific TLVs](#) on page 68
- [IEEE 802.3 organizationally-specific TLVs](#) on page 68
- [Organizationally-specific TLVs for MED devices](#) on page 68

## Management TLVs

The optional management TLVs are as follows:

- Port Description TLV
- System Name TLV
- System Description TLV
- System Capabilities TLV (indicates both the system supported capabilities and enabled capabilities, such as end station, bridge, or router)
- Management Address TLV

## IEEE 802.1 organizationally-specific TLVs

The optional IEEE 802.1 organizationally-specific 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 5000 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-specific 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 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 provide switch information. 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

You can also use the `show sys-info` command to display information about the Inventory TLVs.

### 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 contained in the LLDPDU 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.

Time to live interval

The Time to live interval represents the tx-interval multiplied by the tx-hold-multiplier.

Med fast start

Med fast start provides a burst of LLDPDU when the system initializes an LLDP MED transmission.

---

## 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 have priority over the ADAC configuration on the port.

When you enable Auto QoS, the MED network policy is changed to DSCP 47 (0x2F) from user defined DSCP.

---

## Avaya Automatic QoS enhancement for LLDP-MED

The Avaya Automatic QoS enhancement for LLDP-MED allows Avaya Automatic QoS to set the DSCP, sent by Network Policy TLV for voice traffic application types, to a value that it recognizes. The LLDP compliant IP phone uses the received DSCP when sending voice traffic so that the traffic is recognized by the Avaya Automatic QoS and is prioritized accordingly.

This feature is automatically enabled when Avaya Automatic QoS is enabled on switch.

# Chapter 6: System configuration with ACLI

---

## General switch administration with ACLI

This section outlines the Command Line Interface commands used in general switch administration. It contains information about the following topics:

- [Stack manager](#) on page 73
- [Multiple switch configurations](#) on page 74
- [New Unit Quick Configuration](#) on page 76
- [IP blocking](#) on page 78
- [Assigning and clearing IP addresses](#) on page 79
- [Assigning and clearing IP addresses for specific units](#) on page 84
- [Displaying interfaces](#) on page 85
- [Setting port speed](#) on page 86
- [Testing cables with the Time Domain Reflectometer](#) on page 89
- [Enabling Autotopology](#) on page 90
- [Enabling flow control](#) on page 92
- [Enabling rate-limiting](#) on page 94
- [Using Simple Network Time Protocol](#) on page 96
- [Real time clock configuration](#) on page 102
- [Custom Autonegotiation Advertisements](#) on page 104
- [Connecting to Another Switch](#) on page 106
- [Domain Name Server \(DNS\) Configuration](#) on page 107
- [Auto Unit Replacement using the ACLI](#) on page 110
- [Avaya Energy Saver configuration using the ACLI](#) on page 113
- [Changing switch software in the ACLI](#) on page 122
- [Configuration files in ACLI](#) on page 124
- [Terminal setup](#) on page 130
- [Setting the default management interface](#) on page 131
- [Setting Telnet access](#) on page 131

- [Setting boot parameters](#) on page 134
- [Defaulting to BootP-when-needed](#) on page 135
- [shutdown command](#) on page 136
- [reload command](#) on page 137
- [ACLI Help](#) on page 138
- [Clearing the default TFTP server with ACLI](#) on page 138
- [Configuring a default TFTP server with ACLI](#) on page 139
- [Displaying the default TFTP server with ACLI](#) on page 139
- [Host keys](#) on page 142
- [Secure Transfer File Protocol configuration](#) on page 139
- [Configuring daylight savings time with ACLI](#) on page 146
- [Configuring default clock source with ACLI](#) on page 147
- [Configuring local time zone with ACLI](#) on page 147
- [Configuring Dual Agent with ACLI](#) on page 148
- [Configuring IPv6 with ACLI](#) on page 151
- [Configuring LLDP with ACLI](#) on page 164
- [Configuring PoE detection method with ACLI](#) on page 190
- [Customizing ACLI banner with ACLI](#) on page 194
- [Displaying complete GBIC information](#) on page 196
- [Displaying hardware information](#) on page 196
- [Configuring AUR with ACLI](#) on page 196
- [Agent Auto Unit Replacement \(AAUR\)](#) on page 199
- [Enabling Autosave](#) on page 201
- [Disabling Autosave](#) on page 201
- [Setting Stack Forced Mode](#) on page 202
- [Enabling feature license files](#) on page 203
- [Setting user access limitations](#) on page 204
- [Configuring serial console port and USB host port](#) on page 207
- [Restoring factory default](#) on page 211



---

## Stack manager

Use the following procedures to integrate switches in a stack with the stack manager:

- [Configuring a pure stack with stack manager](#) on page 73
- [Configuring a hybrid stack with stack manager](#) on page 73
- [show stack oper-mode](#) on page 73
- [stack oper-mode {Pure|Hybrid}](#) on page 74

### Configuring a pure stack with stack manager

Use this procedure to configure a pure stack with stack manager.

#### Procedure steps

Upgrade the existing stack with release 6.2 software.

### Configuring a hybrid stack with stack manager

Use this procedure to configure a hybrid stack with stack manager.

#### Procedure steps

1. Upgrade the existing stack with release 6.0 software.
2. Cable in one Ethernet Routing Switch 5600 Series switch into this stack.  
  
Once the new Ethernet Routing Switch 5600 Series switch joins the stack, it will have learned the entire configuration from the base unit and programmed its NVRAM. This switch can now be configured as base unit.
3. To configure the Ethernet Routing Switch 5600 Series switch as the base unit, turn the power off to the whole stack and set the base unit switch on the Ethernet Routing Switch 5500 Series switch to Off and set the base unit switch on the Ethernet Routing Switch 5600 Series switch to On.
4. Turn the power on to the stack. The Ethernet Routing Switch 5600 Series switch is now the base unit in the stack.

You can now add more than one Ethernet Routing Switch 5600 Series switch to the stack. You can add more Ethernet Routing Switch 5600 Series switches to the stack up to the maximum of eight units.

### show stack oper-mode

An Ethernet Routing Switch 5000 Series stack is in one of two modes: Pure or Hybrid.

Use this procedure to display the stack operation mode.

### Procedure steps

Use the following command from Global Configuration mode:

```
show stack oper-mode
```

## stack oper-mode {Pure|Hybrid}

You can configure the operating mode on all the Ethernet Routing Switch 5600 Series switches in the stack. Ethernet Routing Switch 5500 Series switches do not have a configurable operating mode as the software operates in only one mode.

This command is available only on the Ethernet Routing Switch 5600 Series switches in the stack or on an Ethernet Routing Switch 5600 Series stand-alone switch.

Use this procedure to configure the stack as Pure or Mixed.

### Procedure steps


Use the following command from Global Configuration mode:

```
stack oper-mode {Pure|Hybrid}
```

### Variable definitions

The following table defines the parameters for the `stack oper-mode {Pure|Hybrid}` command.

**Table 7: stack oper-mode command parameters**

Variable	Value
Pure	Sets stack manager for an Ethernet Routing Switch 5600 Series stack or stand-alone.
Hybrid	Sets stack manager for a hybrid Ethernet Routing Switch 5600 Series and Ethernet Routing Switch 5600 Series stack.  <b>Note:</b> You must use an Ethernet Routing Switch 5600 Series switch as the base unit in a hybrid or mixed stack.

---

## Multiple switch configurations

The following ACLI commands are used to configure and use multiple switch configuration:

**Navigation:**

- [show nvram block command](#) on page 75
- [copy config nvram block command](#) on page 75
- [copy nvram config block command](#) on page 75

**show nvram block command**

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

**Procedure steps**

Use the following command from Global Configuration mode:

```
show nvram block
```

**copy config nvram block command**

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

**Procedure steps**

Use the following command from Global Configuration mode:

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

**Variable definitions**

The following table describes the parameters for the `copy config nvram block <1-2> name <block_name>` command.

**Table 8: copy config nvram block command parameters**

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

**copy nvram config block command**

Use this procedure to copy the configuration stored in flash memory at the specified location and make it the active configuration.

**Procedure steps**

Use the following command from Global Configuration mode:

```
copy nvram config block <1-2>
```

Substitute <1-2> with the configuration file to load.

This command causes the switch to reset so that the new configuration can be loaded.

---

## New Unit Quick Configuration

In Software Release 4.2 and later, use the New Unit Quick Configuration feature to create a default configuration that can be applied to any new unit entering a stack configuration. You do not need to manually configure a new unit that is added to the existing stack. However, if required, you can set the default values for VLAN Ids, port speed, duplex mode, PVID, tagging, and spanning tree groups on the new unit without the need to reset the stack during the process.

Note: All commands in this section are executed in the Global Configuration command mode except the `quickconfig start-recording` command which is executed in Privileged EXEC mode.

To configure and enable this feature with ACLI, refer to the following commands:

- [quickconfig enable](#) on page 76
- [no quickconfig enable](#) on page 76
- [default quickconfig](#) on page 76
- [quickconfig start-recording](#) on page 77

### quickconfig enable

Use this procedure to enable the quick configuration feature on the switch.

#### Procedure steps

Use the following command from Global Configuration mode:

```
quickconfig enable
```

### no quickconfig enable

Use this procedure to disable the quick configuration feature on the switch.

#### Procedure steps

Use the following command from Global Configuration mode:

```
no quickconfig enable
```

### default quickconfig

Use this procedure to set the quick configuration feature to the factory default value.

## Procedure steps

Use the following command from Global Configuration mode:

```
default quickconfig
```

## quickconfig start-recording

Use this procedure on the stack base unit to record the default configuration that is applied to new units in the stack.

### Procedure steps

1. Use the following command from Global Configuration mode:

```
quickconfig (start-recording)[u3]
```

2. To record a VLAN configuration or port configuration enter the following commands one on each line in ACLI:

```
enable
config term
vlan port $/13-40 tag untagPvidonly
vlan create 10 name vlan_10 type port
vlan create 20 name vlan_20 type port
vlan members add 10 $/13-40
vlan members add 20 $/13-40
vlan ports $/13-40 pvid 10
interface fast $/13-34
speed 100
end
.
```

### Caution:

The first two commands must be **enable** and **config term**, otherwise the **config** commands that follow will not be applied.

Use **\$** as a wild card for the slot. When you add a new unit to the stack the unit number is not known so the wild card character can match any slot number. To end the recording process enter a dot on a separate line in ACLI.

## IP blocking

IP blocking provides a safeguard against the use of duplication IP addresses in a stack at the Layer 3 level. When a unit leaves a stack or reboots the IP blocking feature ensures that duplicate IPs are not present.

Use the following ACLI commands to configure and manage IP blocking with ACLI:

- [show ip-blocking](#) on page 78
- [show ip blocking-mode](#) on page 78
- [ip blocking-mode command](#) on page 78
- [clear ip-blocking](#) on page 79
- [default ip blocking-mode](#) on page 79

### show ip-blocking

Use this procedure to show the current IP blocking state.

#### Procedure steps

Use the following command from User EXEC mode:

```
show ip-blocking
```

### show ip blocking-mode

Use this procedure to show the current IP blocking parameters.

#### Procedure steps

Use the following command from User EXEC mode:

```
show ip blocking-mode
```

### ip blocking-mode command

Use this procedure to set the level of ip blocking to perform in the stack.

#### Procedure steps

Use the following command from Interface Configuration mode:

```
ip blocking-mode {full | none}
```

### Variable definitions

The following table describes the parameters for the `ip blocking-mode {full | none}` command.

**Table 9: ip blocking-mode command parameters**

Variable	Value
full	Select this parameter to set IP blocking-mode to full. This never enables a duplicate IP address in a stack.
none	Select this parameter to set IP blocking-mode to none. This enables duplicate IP addresses unconditionally.

## clear ip-blocking

Use this procedure to clear the current IP blocking-mode state.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
clear ip-blocking
```

## default ip blocking-mode

Use this procedure to set the IP blocking mode to factory defaults.

### Procedure steps

Use the following command from Global Configuration mode:

```
default ip blocking-mode
```

---

## Assigning and clearing IP addresses

You can assign, clear, and view IP addresses and gateway addresses with ACLI. Use the following commands to perform various operations on IP and gateway addresses:

- [ip address command](#) on page 80
- [ip address source command](#) on page 80
- [no ip address command](#) on page 81
- [ip default-gateway command](#) on page 82

- [no ip default-gateway command](#) on page 82
- [show ip command](#) on page 83

## ip address command

Use this procedure to set the IP address and subnet mask for the switch or a stack.

### Procedure steps

Use the following command from Global Configuration mode:

```
ip address [stack | switch] <A.B.C.D> [netmask <A.B.C.D>]
[default-gateway <A.B.C.DX>]
```

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 stand-alone mode.

### Variable definitions

The following table describes the parameters for the `ip address [stack | switch] <A.B.C.D> [netmask <A.B.C.D>][default-gateway <A.B.C.DX>]` command.

**Table 10: ip address command parameters**

Variable	Value
stack   switch	Sets the IP address and netmask of the stack or the switch.
A.B.C.D	Denotes the IP address in dotted-decimal notation; netmask is optional.
netmask	Signifies the IP subnet mask for the stack or switch.
Default Gateway A.B.C.D	Displays the IP address of the default gateway. Enter the IP address of the default IP gateway.

#### \* Note:

When the IP address or subnet mask is changed, connectivity to Telnet can be lost.

## ip address source command

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

### Procedure steps

Use the following command from Global Configuration mode:



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

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

### Variable definitions

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

**Table 11: ip address source command parameters**

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

## no ip address command

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

### Procedure steps

Use the following command from Global Configuration mode:

```
no ip address {stack | switch | unit}
```

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

### Variable definitions

The following table describes the parameters for the `no ip address {stack | switch | unit}` command.

**Table 12: no ip address command parameters**

Variable	Value
stack   switch	Zeroes out the stack IP address and subnet mask or the switch IP address and subnet mask.

Variable	Value
unit	Zeroes out the IP address for the specified unit.

**\* Note:**

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

## ip default-gateway command

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

### Procedure steps

Use the following command from Global Configuration mode:

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

### Variable definitions

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

**Table 13: ip default-gateway command parameters**

Variable	Value
A.B.C.D	Enter the dotted-decimal IP address of the default IP gateway.

**\* Note:**

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

## no ip default-gateway command

Use this procedure to set the IP default gateway address to zero (0).

### Procedure steps

Use the following command from Global Configuration mode:

```
no ip default-gateway
```

**\* Note:**

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

## show ip command

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

### Procedure steps

Use the following command from User EXEC mode:

```
show ip [bootp] [dhcp] [default-gateway] [address]
```

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

### Variable definitions

The following table describes the parameters and variables for the `show ip` command.

**Table 14: show ip command parameters**

Variable	Value
<code>bootp</code>	Displays BootP/DHCP-related IP information. The possibilities for status returned are: <ul style="list-style-type: none"> <li>• BootP Always</li> <li>• Disabled</li> <li>• BootP or Last Address</li> <li>• BootP When Needed</li> <li>• DHCP Always</li> <li>• DHCP or Last Address</li> <li>• DHCP When Needed</li> </ul>
<code>dhcp client lease</code>	Displays DHCP client lease information. The command displays information about configured lease time and lease time granted by the DHCP server.
<code>default-gateway</code>	Displays the IP address of the default gateway.
<code>address</code>	Displays the current IP address.
<code>address source</code>	Displays the BootP or DHCP client information. The possibilities for status returned are: <ul style="list-style-type: none"> <li>• DHCP always</li> <li>• DHCP when needed</li> <li>• DHCP or last address</li> <li>• Disabled</li> </ul>

Variable	Value
	<ul style="list-style-type: none"> <li>• BootP always</li> <li>• BootP when needed</li> <li>• BootP or last address</li> </ul>

## 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, refer to the following:

- [ip address unit command](#) on page 84
- [no ip address unit command](#) on page 84
- [default ip address unit command](#) on page 85

### ip address unit command

Use this procedure to set the IP address and subnet mask of a specific unit in the stack.

#### Procedure steps

Use the following command from Global Configuration mode:

```
ip address unit <1-8> [A.B.C.D]
```

#### Variable definitions

The following table describes the parameters the `ip address unit <1-8> [A.B.C.D]` command.

**Table 15: ip address unit command parameters**

Variable	Value
<code>unit &lt;1-8&gt;</code>	Sets the unit you are assigning an IP address.
<code>A.B.C.D</code>	Enter IP address in dotted-decimal notation.

#### \* Note:

When the IP address or subnet mask is changed, connectivity to Telnet and the Internet can be lost.

### no ip address unit command

Use this procedure to set the IP address for the specified unit in a stack to zeros (0).

## Procedure steps

Use the following command from Global Configuration mode:

```
no ip address unit <1-8>
```

### Variable definitions

The following table describes the parameters the `no ip address unit <1-8>` command.

**Table 16: no ip address command parameters**

Variable	Value
unit <1-8>	Zeroes out the IP address for the specified unit.

**\* Note:**

When the IP address or subnet mask is changed, connectivity to Telnet and the Internet can be lost.

## default ip address unit command

Use this procedure to set the IP address for the specified unit in a stack to all zeros (0).

### Procedure steps

Use the following command from Global Configuration mode:

```
default ip address unit <1-8>
```

### Variable definitions

The following table describes the parameters for the `default ip address unit <1-8>` command.

**Table 17: default ip address unit command parameters**

Variable	Value
unit <1-8>	Zeroes out the IP address for the specified unit.

**\* Note:**

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

---

## Displaying interfaces

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

## show interfaces command

Use this procedure to display the current configuration and status of all interfaces.

### Procedure steps

Use the following command from User EXEC mode:

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

### Variable definitions

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

**Table 18: show interfaces command parameters**

Value	Variable
names <portlist>	Displays the interface names; enter specific ports if you want to see only those.

---

## Setting port speed

To set port speed and duplexing with ACLI, refer to the following:

- [speed command](#) on page 86
- [default speed command](#) on page 87
- [duplex command](#) on page 88
- [default duplex command](#) on page 88

## speed command

Use this procedure to set the speed of the port.

### Procedure steps

Use the following command from Interface Configuration mode:

```
speed [port <portlist>] {10 | 100 | 1000 | auto}
```

### Variable definitions

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

**Table 19: speed command parameters**

Variable	Value
<code>port &lt;portlist&gt;</code>	Specifies the port numbers for which to configure the speed. Enter the port numbers you want to configure.  * <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the <b>interface</b> command.
<code>10   100   1000   auto</code>	Sets speed to: <ul style="list-style-type: none"> <li>• 10--10 Mb/s</li> <li>• 100--100 Mb/s</li> <li>• 1000--1000 Mb/s or 1 GB/s</li> <li>• auto--autonegotiation</li> </ul>

\* **Note:**

Enabling/disabling autonegotiation for speed also enables/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

Use this procedure to set the speed of the port to the factory default speed.

### Procedure steps

Use the following command from Interface Configuration mode:

```
default speed [port <portlist>]
```

### Variable definitions

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

**Table 20: Default speed command parameters**

Variable	Value
<code>port &lt;portlist&gt;</code>	Specifies the port numbers to set the speed to factory default. Enter the port numbers you want to set.  * <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the <b>interface</b> command.

## duplex command

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

### Procedure steps

Use the following command from Interface Configuration mode:

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

### Variable definitions

The following table describes the parameters for the `duplex [port <portlist>] {full | half | auto}` command.

**Table 21: Duplex command parameters**

Variable	Value
<code>port &lt;portlist&gt;</code>	Specifies the port numbers for which to reset the duplex mode to factory default values. Enter the port number you want to configure. The default value is autonegotiation.  * <b>Note:</b> If you omit this parameter, the system uses the ports you specified in the <b>interface</b> command.
<code>full   half   auto</code>	Sets duplex to: <ul style="list-style-type: none"> <li>• full--full-duplex mode</li> <li>• half--half-duplex mode</li> <li>• auto--autonegotiation</li> </ul>

\* **Note:**

Enabling/disabling autonegotiation for speed also enables/disables it for duplex operation.

When you set the duplex mode for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

## default duplex command

Use this procedure to set the duplex operation for a port to the factory default duplex value.

### Procedure steps

Use the following command from Interface Configuration mode:



```
default duplex [port <portlist>]
```

### Variable definitions

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

**Table 22: Default duplex command parameters**

Variable	Value
port <portlist>	<p>Specifies the port numbers to reset the duplex mode to factory default values. Enter the port numbers you want to configure. The default value is autonegotiation.</p> <p><b>* Note:</b> If you omit this parameter, the system uses the ports you specified in the <code>interface</code> command.</p>

## Testing cables with the Time Domain Reflectometer

The Avaya Ethernet Routing Switch 5000 Series is equipped with a Time Domain Reflectometer (TDR). The TDR provides a diagnostic capability to test connected cables for defects (such as short pin and pin open). You can obtain TDR test results from ACLI or Enterprise Device Manager.

The cable diagnostic tests only apply to Ethernet copper ports; fiber ports cannot be tested.

You can initiate a test on multiple ports at the same time.

When you test a cable with the TDR, if the cable has a 10/100 MB/s link, the link is broken during the test and restored only when the test is complete. If the cable has a 10/100 MB/s link, the test results may be incomplete as the test does not test all of the pins in the connector. Use of the TDR does not affect 1 GB/s links.

See the *Avaya Ethernet Routing Switch Troubleshooting Guide (NN47200-700)* for more information on troubleshooting cables and for connector pin tables.

**\* Note:**

The accuracy margin of cable length diagnosis is between three to five meters. Avaya suggests the shortest cable for length information be five meters long.

With the following ACLI commands, you can initiate a TDR cable diagnostic test and obtain test reports.

- [tdr test command](#) on page 89
- [show tdr command](#) on page 90

### tdr test command

Use this procedure to initiate a TDR test on a port or ports.

## Procedure steps

Use the following command from Privileged EXEC mode:

```
tdr test <portlist>
```

### Variable definitions

The following table describes the parameters for the `tdr test <portlist>` command.

**Table 23: Tdr test command parameters**

Variable	Value
<portlist>	Specifies the ports to be tested.

## show tdr command

Use this procedure to display the results of a TDR test.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
show tdr <portlist>
```

### Variable definitions

The following table describes the parameters for the `show tdr <portlist>` command.

**Table 24: Show tdr command parameters**

Variable	Value
<portlist>	Specifies the ports for which to display the test results.

---

## Enabling Autotopology

The Optivity Autotopology protocol can be configured with ACLI.

For more information about Autotopology, refer to [www.avaya.com](http://www.avaya.com). (The product family for Optivity and Autotopology is Data and Internet.)

To enable autotopology with ACLI, refer to the following:

- [autotopology command](#) on page 91
- [no autotopology command](#) on page 91
- [default autotopology command](#) on page 91
- [show autotopology settings command](#) on page 91
- [show autotopology nmm-table command](#) on page 92

## autotopology command

Use this procedure to enable the Autotopology protocol.

### Procedure steps

Use the following command from Global Configuration mode:

```
autotopology
```

## no autotopology command

Use this procedure to disable the Autotopology protocol.

### Procedure steps

Use the following command from Global Configuration mode:

```
no autotopology
```

## default autotopology command

Use this procedure to enable the Autotopology protocol.

### Procedure steps

Use the following command from Global Configuration mode:

```
default autotopology
```

**\* Note:**

The `default autotopology` command has no parameters or values.

## show autotopology settings command

Use this procedure to display the global autotopology settings.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
show autotopology settings
```

**\* Note:**

The `show autotopology settings` command has no parameters or values.

## show autotopology nmm-table command

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

### Procedure steps

Use the following command from Privileged EXEC mode:

```
show autotopology nmm-table
```

**\* Note:**

The `show autotopology nmm-table` command has no parameters or values.

## Enabling flow control

Gigabit Ethernet, when used with the Avaya Ethernet Routing Switch 5000 Series, can control traffic on this port using the `flowcontrol` command.

To enable flow control with ACLI, refer to the following:

- [flowcontrol command](#) on page 92
- [no flowcontrol command](#) on page 93
- [default flowcontrol command](#) on page 93

## flowcontrol command

Use this procedure to control the traffic rates during congestion.

### Procedure steps

Use the following command from Interface Configuration mode:

```
flowcontrol [port <portlist>] {asymmetric | symmetric | auto | disable}
```

**\* Note:**

This command is used only on Gigabit Ethernet ports.

### Variable definitions

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

**Table 25: Flowcontrol command parameters**

Variable	Value
port <portlist>	Specifies the port numbers to configure for flow control.

Variable	Value
	<p><b>* Note:</b></p> <p>If you omit this parameter, the system uses the ports you specified in the <b>interface</b> command but only those ports which have speed set to 1000/full.</p>
<pre>asymmetric   symmetric   auto   disable</pre>	<p>Sets the mode for flow control:</p> <ul style="list-style-type: none"> <li>• asymmetric--PAUSE frames can only flow in one direction.</li> <li>• symmetric--PAUSE frames can flow in either direction.</li> <li>• auto--sets the port to automatically determine the flow control mode (default).</li> <li>• disable--disables flow control on the port.</li> </ul>

## no flowcontrol command

Use this procedure to disable flow control.

### Procedure steps

Use the following command from Interface Configuration mode:

```
no flowcontrol [port <portlist>]
```

**\* Note:**

This command is used only on Gigabit Ethernet ports.

### Variable definitions

The following table describes the parameters for the **no flowcontrol** command.

**Table 26: No flowcontrol command parameters**

Variable	Value
<pre>port &lt;portlist&gt;</pre>	<p>Specifies the port numbers for which to disable flow control.</p> <p><b>* Note:</b></p> <p>If you omit this parameter, the system uses the ports you specified in the <b>interface</b> command, but only those ports that have speed set to 1000/full.</p>

## default flowcontrol command

Use this procedure to set the flow control to auto, which automatically detects the flow control.

## Procedure steps

Use the following command from Interface Configuration mode:

```
default flowcontrol [port <portlist>]
```

**\* Note:**

This command is used only on Gigabit Ethernet ports.

## Variable definitions

The following table describes the parameters for the `default flowcontrol` command.

**Table 27: Default flowcontrol command parameters**

Variable	Value
<code>port &lt;portlist&gt;</code>	Specifies the port numbers to default to auto flow control.  <b>* Note:</b> If you omit this parameter, the system uses the port number you specified in the <code>interface</code> command.

---

## Enabling rate-limiting

The percentage or packets per seconds of multicast traffic, or broadcast traffic, or both can be limited with ACLI. For details, refer to the following:

- [show rate-limit command](#) on page 94
- [rate-limit command](#) on page 94
- [no rate-limit command](#) on page 95
- [default rate-limit command](#) on page 96

### show rate-limit command

Use this procedure to display the rate-limiting settings and statistics.

#### Procedure steps

Use the following command from Privileged EXEC mode:

```
show rate-limit
```

### rate-limit command

Use this procedure to configure rate-limiting on the port.

## Procedure steps

Use the following command from Interface Configuration mode:

```
rate-limit {multicast | broadcast | both } {percent <0-10> | pps
<0-262143 / <0-10>}
```

## Variable definitions

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

**Table 28: Rate-limit command parameters**

Variable	Value
multicast   broadcast   both	Applies rate-limiting to the type of traffic. <ul style="list-style-type: none"> <li>• multicast--applies rate-limiting to multicast packets</li> <li>• broadcast--applies rate-limiting to broadcast packets</li> <li>• both--applies rate-limiting to both multicast and broadcast packets</li> </ul>
percent <0-10>   pps <0-262143>	Specifies the mode for setting the rates of the incoming traffic. <ul style="list-style-type: none"> <li>• percent &lt;0-10&gt;--enter an integer from 1 to 10 to set the rate-limiting percentage.</li> <li>• pps &lt;0-262143&gt;--enter an integer from 1 to 262143 to set the rate-limiting packets per second.</li> </ul> <p>For 10 Gb/s links, the default value for limiting both broadcast and multicast is 10 percent.</p> <p>When pps mode is used the limit on 10 Gb/s links cannot be configured to a value under 1000.</p> <p>Rate limiting using packet per seconds can only be configured using ACLI.</p>

## no rate-limit command

Use this procedure to disable rate-limiting on the port.

## Procedure steps

Use the following command from Interface Configuration mode:

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

## Variable definitions

The following table describes the parameters for the `no rate-limit` command.

**Table 29: No rate-limit command parameters**

Variable	Value
<code>port &lt;portlist&gt;</code>	Specifies the port numbers to disable for rate-limiting. Enter the port numbers you want to disable.  * <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the <b>interface</b> command.

## default rate-limit command

Use this procedure to restore the rate-limiting value for the specified port to the default setting.

### Procedure steps

Use the following command from Interface Configuration mode:

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

### Variable definitions

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

**Table 30: Default rate-limit command parameters**

Variable	Value
<code>port &lt;portlist&gt;</code>	Specifies the port numbers on which to reset rate-limiting to factory default. Enter the port numbers on which to set rate-limiting to default.  * <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the <b>interface</b> command.

---

## Using Simple Network Time Protocol

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

### \* **Note:**

If you have trouble using 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.

Using SNTP provides a real-time timestamp for the software, shown as Greenwich Mean Time (GMT).

If SNTP is enabled, the system synchronizes with the configured NTP server at boot-up and at user-configurable periods thereafter (the default synchronization interval is 24 hours). The first synchronization is not performed until network connectivity is established.

SNTP supports primary and secondary NTP servers. The system tries the secondary NTP server only if the primary NTP server is unresponsive.

To configure SNTP, refer to the following commands:

- [show SNTP command](#) on page 97
- [show sys-info command](#) on page 97
- [SNTP enable command](#) on page 98
- [no SNTP enable command](#) on page 98
- [SNTP server primary address command](#) on page 98
- [SNTP server secondary address command](#) on page 99
- [no SNTP server command](#) on page 99
- [SNTP sync-now command](#) on page 99
- [SNTP sync-interval command](#) on page 100
- [Configuring the local time zone](#) on page 100
- [Configuring daylight savings time](#) on page 101

## show SNTP command

Use this procedure to display the SNTP information, as well as the configured NTP servers.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
show SNTP
```

## show sys-info command

Use this procedure to display the current system characteristics.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
show sys-info
```

**\* Note:**

You must have SNTP enabled and configured to display GMT time.

## SNTP enable command

Use this procedure to enable SNTP.

### Procedure steps

Use the following command from Global Configuration mode:

```
SNTP enable
```

**\* Note:**

The default setting for SNTP is disabled.

## no SNTP enable command

Use this procedure to disable SNTP.

### Procedure steps

Use the following command from Global Configuration mode:

```
no SNTP enable
```

## SNTP server primary address command

Use this procedure to specify the IP addresses of the primary NTP server.

### Procedure steps

Use the following command from Global Configuration mode:

```
sntp server primary address [<ipv6_address> | <A.B.C.D>]
```

### Variable definitions

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

**Table 31: SNTP server primary address command parameters**

Variable	Value
<A.B.C.D>	Enter the IP address of the primary NTP server in dotted-decimal notation.

## SNTP server secondary address command

Use this procedure to specify the IP addresses of the secondary NTP server.

### Procedure steps

Use the following command from Global Configuration mode:

```
sntp server secondary address [<ipv6_address> | <A.B.C.D>]
```

### Variable definitions

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

**Table 32: SNTP server secondary address command parameters**

Variable	Value
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

Use this procedure to clear the NTP server IP addresses. The command clears the primary and secondary server addresses.

### Procedure steps

Use the following command from Global Configuration mode:

```
no sntp server {primary | secondary}
```

### Variable definitions

The following table describes the parameters for the `no sntp server` command.

**Table 33: no SNTP server command parameters**

Variable	Value
primary	Clear primary SNTP server address.
secondary	Clear secondary SNTP server address.

## SNTP sync-now command

Use this procedure to force a manual synchronization with the NTP server.

## Procedure steps

Use the following command from Global Configuration mode:

```
Sntp sync-now
```

**\* Note:**

Sntp must be enabled before this command can take effect.

## Sntp sync-interval command

Use this procedure to specify recurring synchronization with the secondary NTP server in hours relative to initial synchronization.

### Procedure steps

Use the following command from Global Configuration mode:

```
sntp sync-interval <0-168>
```

### Variable definitions

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

**Table 34: Sntp sync-interval command parameters**

Variable	Value
<0-168>	Enter the number of hours for periodic synchronization with the NTP server.  <b>* Note:</b> 0 is boot-time only, and 168 is once a week.

## Configuring the local time zone

Use this procedure to configure your switch for your local time zone.

### Procedure steps

1. Use the following command from Global Configuration mode:

```
configure
```

2. Enable sntp server.

3. Set clock time zone using the clock command.

```
clock time-zone zone hours [minutes]
```

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."

### Variable definitions

The following table describes the parameters for the `clock time-zone zone hours [minutes]` command.

**Table 35: clock time-zone command parameters**

Variable	Value
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.

## Configuring daylight savings time

Use this procedure to configure local daylight savings time recurring change dates.

1. Use the following command from Global Configuration mode:

```
configure
```

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]
```

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.

### Variable definitions

The following table describes the parameters for the `clock summer-time zone date day month year hh:mm day month year hh:mm [offset]` command

**Table 36: daylight savings command parameters**

Variable	Value
date	Indicates that daylight savings time should 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.

---

## Real time clock configuration

In addition to SNTP time configuration, a real-time clock (RTC) is available to provide the switch with time information. This RTC provides the switch information in the instance that SNTP time is not available.

Use the following commands to view and configure the RTC:

- [clock set command](#) on page 102
- [Clock sync-rtc-with-SNTP enable command](#) on page 103
- [no clock sync-rtc-with-SNTP enable](#) on page 103
- [Default clock sync-rtc-with-SNTP enable](#) on page 104
- [Clock source command](#) on page 104
- [default clock source](#) on page 104

### clock set command

Use this procedure to set the RTC. The syntax of the clock set.

**\* Note:**

The clock set command is only applicable for 5530 and 56XX.

**Procedure steps**

Use the following command from Privileged EXEC mode:

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

**Variable definitions**

The following table outlines the parameters for the `clock set {<LINE> | <hh:mm:ss>}` command.

**Table 37: clock set command parameters**

Variable	Value
<LINE>	A string in the format of mmddyyhhmmss that defines the current local time.
<hh:mm:ss>	Numeric entry of the current local time in the manner specified.

**Clock sync-rtc-with-SNTP enable command**

Use this procedure to enable the syncing of the RTC with the SNTP clock when the SNTP clock synchronizes.

**\* Note:**

The clock sync-rtc-with-SNTP enable command is only applicable for 5530 and 56XX.

**Procedure steps**

Use the following command from Global Configuration mode:

```
clock sync-rtc-with-sntp enable
```

**no clock sync-rtc-with-SNTP enable**

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

**Procedure steps**

Use the following command from Global Configuration mode:

```
no clock sync-rtc-with-sntp enable
```

## Default clock sync-rtc-with-SNTP enable

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

### Procedure steps

Use the following command from Global Configuration mode:

```
default clock sync-rtc-with-sntp enable
```

## Clock source command

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

### Procedure steps

Use the following command from Global Configuration mode:

```
clock source {sntp | rtc | sysUpTime}
```

Substitute {sntp | rtc | sysUpTime} with the clock source selection.

## default clock source

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

### Procedure steps

Use the following command from Global Configuration mode:

```
default clock source
```

---

## Custom Autonegotiation Advertisements

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

The following sections describe configuring CANA with ACLI:

- [Configuring CANA](#) on page 105
- [Viewing current autonegotiation advertisements](#) on page 50
- [Viewing hardware capabilities](#) on page 105



- [Setting default auto-negotiation-advertisements](#) on page 105
- [no auto-negotiation-advertisements command](#) on page 106

## Configuring CANA

Use this procedure to configure CANA.

### Procedure steps

Use the following command from Global Configuration mode:

```
auto-negotiation-advertisements
```

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

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

## Viewing current autonegotiation advertisements

Use this procedure to view the autonegotiation advertisements for the device.

### Procedure steps

Use the following command from Global Configuration mode:

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

## Viewing hardware capabilities

Use this procedure to view the available operational modes for the device.

### Procedure steps

Use the following command from Interface Configuration mode:

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

## Setting default auto-negotiation-advertisements

Use this procedure to make a port advertise all its auto-negotiation-capabilities.

### Procedure steps

Use the following command from Interface Configuration mode:

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

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

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

## no auto-negotiation-advertisements command

Use this procedure to make a port silent.

### Procedure steps

Use the following command from Interface Configuration mode:

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

---

## Connecting to Another Switch

Using the Command Line Interface (CLI), it is possible to communicate with another switch while maintaining the current switch connection. This is accomplished with the familiar `ping` and `telnet` commands.

## ping command

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

### Procedure steps

Use the following command from User EXEC mode:

```
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.

### Variable definitions

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

**Table 38: ping command parameters**

Variable	Value
<code>&lt;ipv6_address   dns_host_name&gt;</code>	The IPv6 address or the DNS host name of the unit to test.
<code>datasize &lt;64-4096&gt;</code>	Specify the size of the ICMP packet to be sent. The data size range is from 64 to 4096 bytes.

Variable	Value
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 <i>timeout</i> with the <i>-t</i> 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 this procedure to establish communications with another switch during the current ACLI session.

### Procedure steps

Use the following command from User EXEC mode:

```
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.

Communication can be established to only one external switch at a time using the `telnet` command.

---

## Domain Name Server (DNS) Configuration

Domain name servers are used when the switch needs to resolve a domain name (such as "avaya.com") to an IP address. The following commands allow for the configuration of the switch domain name servers:

- [show ip dns command](#) on page 108
- [ip domain-name command](#) on page 108
- [no ip domain-name command](#) on page 108
- [default ip domain-name command](#) on page 108
- [ip name-server command](#) on page 109
- [no ip name-server command](#) on page 110

## show ip dns command

Use this procedure to display DNS-related information.

### Procedure steps

Use the following command from User EXEC mode:

```
show ip dns
```

**\* Note:**

This information includes the default switch domain name and any configured DNS servers.

## ip domain-name command

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

### Procedure steps

Use the following command from Global Configuration mode:

```
ip domain-name <domain_name>
```

Substitute <domain\_name> with the default domain name to be used. A domain name is determined to be valid if it contains alphanumeric characters and contains at least one period (.).

**\* Note:**

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

## no ip domain-name command

Use this procedure to clear a previously configured default DNS domain name for the switch.

### Procedure steps

Use the following command from Global Configuration mode:

```
no ip domain-name
```

## default ip domain-name command

Use this procedure to set the system default switch domain name.

## Procedure steps

Use the following command from Global Configuration mode:

```
default ip domain-name
```

**\* Note:**

Because this default is an empty string, this command has the same effect as the `no ip domain-name` command.

## ip name-server command

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

### Procedure steps

Use the following command from Global Configuration mode:

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

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

**\* Note:**

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

### Variable definitions

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

**Table 39: ip name-server command parameters**

Variable	Value
<code>ipv6_address</code>	The IPv6 address of the domain name server used by the switch.
<code>&lt;ip_address_1&gt;</code>	The IP address of the domain name server used by the switch.
<code>&lt;ip_address_2&gt;</code>	Optional. The IP address of a domain name server to add to the list of servers used by the switch.
<code>&lt;ip_address_3&gt;</code>	Optional. The IP address of a domain name server to add to the list of servers used by the switch.

## no ip name-server command

Use this procedure to remove domain name servers from the list of servers used by the switch to resolve domain names to an IP address.

### Procedure steps

Use the following command from Global Configuration mode:

```
no ip name-server <ip_address_1> no ip name-server
[<ip_address_2>] no ip name-server [<ip_address_3>]
```

**Note:**

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

### Variable definitions

The following table outlines the parameters for the `no ip name-server` command.

**Table 40: no ip name-server command parameters**

Variable	Value
<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.

---

## Auto Unit Replacement using the CLI

The following sections describe Auto Unit Replacement (AUR).

---

## Prerequisites

- The units must be in a stack.

---

## Auto Unit Replacement using the ACLI navigation

- [Viewing Auto Unit Replacement using the ACLI](#) on page 111
- [Enabling Auto Unit Replacement using the ACLI](#) on page 112
- [Disabling AUR using the ACLI](#) on page 112
- [Restoring the default setting for AUR using the ACLI](#) on page 112
- [Configuring AUR operation settings using the ACLI](#) on page 112

---

## Viewing Auto Unit Replacement using the ACLI

View Unit Replacement (AUR) to understand the current setting and to discover if the unit is ready for replacement.

### Procedure steps

Use the following command from the privileged EXEC mode:

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

### Job aid

The following table describes the fields for the `show stack auto-unit-replacement` command.

**Table 41: show stack auto-unit-replacement fields**

Field	Description
Auto Unit Replacement Auto-Restore	Specifies whether the Auto Unit Replacement Auto-Restore is enabled for the stack.
Auto Unit Replacement Auto-Save	Specifies whether the Auto Unit Replacement Auto-Save is enabled for the stack.
UNIT #	Specifies the number of the unit in the stack.

Field	Description
READY FOR REPLACEMENT	Specifies whether the unit is ready for replacement.

---

## Enabling Auto Unit Replacement using the ACLI

Enable Unit Replacement (AUR) to permit the automatic update of a license for any stack unit, including the base unit.

### Procedure steps

Use the following command from the Global Configuration mode:

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

**!** Important:

The default mode is enable.

---

## Disabling AUR using the ACLI

Disable AUR to stop the automatic update of a license for any stack unit, including the base unit.

### Procedure steps

Use the following command from the Global Configuration mode:

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

---

## Restoring the default setting for AUR using the ACLI

Restore the default setting for AUR to permit the automatic update of a license for any stack unit, including the base unit.

### Procedure steps

Use the following command from the Global Configuration mode:

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

---

## Configuring AUR operation settings using the ACLI

Configure AUR to modify the operation settings.



## Procedure steps

1. Restore the configuration of a unit from the saved configuration on the base unit by using the following command in Global Configuration mode:

```
stack auto-unit-replacement config restore unit <1-8>
```

2. Force an immediate save of the new base unit (NBU) configuration to the base unit (BU) by using the following command in Global Configuration mode:

```
stack auto-unit-replacement config save unit <1-8>
```

3. Enable AUR auto save by using the following command in Global Configuration mode:

```
stack auto-unit-replacement config save enable
```

4. Disable AUR auto save by using the following command in Global Configuration mode:

```
stack auto-unit-replacement config save disable
```

## Variable definitions

The following table explains the parameters for the `stack auto-unit-replacement config {restore unit <1-8>|save {enable|disable|unit <1-8>}}` command.

**Table 42: stack auto-unit-replacement config parameters**

Variable	Value
disable	Disables AUR auto save.
enable	Enables AUR auto-save.
restore	Restores the configuration of a unit from the saved configuration on the base unit by
save	Forces an immediate save of the NBU configuration to the BU.
unit <1-8>	Identifies the unit in the stack.

---

## Avaya Energy Saver configuration using the ACLI

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

---

## AES configuration using the ACLI navigation

- [Configuring global AES using the ACLI](#) on page 114
- [Configuring port-based AES using the ACLI](#) on page 116
- [Activating or deactivating AES manually using the ACLI](#) on page 116
- [Configuring AES scheduling using the ACLI](#) on page 117
- [Disabling AES scheduling using the ACLI](#) on page 118
- [Configuring AES scheduling to default using the ACLI](#) on page 119
- [Viewing AES scheduling using the ACLI](#) on page 120
- [Viewing AES savings using the ACLI](#) on page 120
- [Viewing the global AES configuration using ACLI](#) on page 120
- [Viewing port-based AES configuration using the ACLI](#) on page 121

---

## Configuring global AES using the ACLI

Use the following procedure to enable or disable the energy saving feature for the switch. Avaya recommends disabling AES on uplink copper ports since activating or deactivating AES on copper ports will trigger a link down followed rapidly by a link up event. The best solution is to use fiber ports for uplinks since link status will not change when AES is activated or deactivated.

**! Important:**

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

**! Important:**

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

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

**! Important:**

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

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

## Procedure steps

Use the following command from Global Configuration mode:

```
[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	<p>Enables AES efficiency mode.</p> <p><b>! Important:</b> You must ensure that SNTP is enabled before you can enable AES efficiency mode.</p> <p><b>! Important:</b> You must disable AES globally before you can modify AES efficiency mode.</p> <p><b>! Important:</b> 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.</p>
enable	Enables AES globally.
[no]	Disables AES efficiency mode, POE power saving, or AES globally.
poe-power-saving	<p>Enables POE power saving.</p> <p><b>! Important:</b> You must disable AES globally before you can modify POE power saving.</p>

---

## Configuring port-based AES using the 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.

### Procedure steps

Use the following command from Interface Configuration mode:

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

### Variable definitions

The following table defines optional parameters that you enter after the `[default] [no] energy-saver 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 the 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 in ACLI.

## Procedure steps

1. Activate AES by using the following command from Privileged EXEC mode:  

```
energy-saver activate
```
2. Deactivate AES by using the following command from Privileged EXEC mode:  

```
energy-saver deactivate
```

---

## Configuring AES scheduling using the 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

- Disable AES globally.

## Procedure steps

Configure AES scheduling by using the following command from Global Configuration mode:

```
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.

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

---

## Disabling AES scheduling using the ACLI

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

### Prerequisites

- Disable AES globally.

### Procedure steps

Configure AES scheduling by using the following command from the Global Configuration mode:

```
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.
weekday	Disables AES scheduling for all weekdays.

Variable	Value
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 the ACLI

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

### Prerequisites

- Disable NES globally.

### Procedure steps

Configure AES scheduling by using the following command from Global Configuration mode:

```
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 the ACLI

Use the following procedure to review configured energy saving schedule information.

### Procedure steps

View AES savings by using the following command from User EXEC mode.

```
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.

```
5650TD-PWR(config)#show energy-saver schedule
Day      Time  Action
-----
Monday   01:01 Activate
Tuesday  01:01 Activate
Wednesday 01:01 Activate
Thursday  01:01 Activate
Friday   01:01 Activate
```

Figure 16: show energy-saver schedule command output

---

## Viewing AES savings using the ACLI

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

### Procedure steps

View AES savings by using the following command from User EXEC mode:

```
show energy-saver savings
```

---

## 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 from User EXEC mode:

```
show energy-saver
```

## Job aid: show energy-saver command output

The following figure displays sample output for the `show energy-saver` command.

```
5530-24TFD(config)#show energy-saver
Avaya Energy Saver (AES): Enabled
AES PoE Power Saving Mode: Disabled
AES Efficiency-Mode Mode: Disabled
Day/Time: Not set
Current AES state: AES is Inactive
```

Figure 17: show energy-saver command output

---

## Viewing port-based AES configuration using the 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
```

## 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.

```
5650TD-PWR(config-if)#show energy-saver interface
Port      AES State PoE Savings PoE Priority
-----
1         Enabled  Enabled  Low
2         Disabled Disabled  Low
3         Enabled  Enabled  Low
4         Disabled Disabled  Low
5         Enabled  Enabled  Low
6         Disabled Disabled  Low
7         Disabled Disabled  Low
8         Disabled Disabled  Low
9         Disabled Disabled  Low
```

Figure 18: show energy-saver interface command output

---

## Changing switch software in the ACLI

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

### Procedure steps

1. Use the following command from User EXEC mode:

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

2. Press Enter.

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

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

The following table shows an example of this message.

**Table 43: Software download message output**

Download Image [//]
Saving Image [-]
Finishing Upgrading Image

During the download process the switch is not operational.

The progress of the download process can be tracked by observing the front panel LEDs. For more information about this topic, refer to [LED activity during software download](#) on page 24.

---

## Variable definitions

The following table outlines the parameters for the `download` command.

**Table 44: download command parameters**

Variable	Value
address <ipv6_address>   <a.b.c.d>	This parameter is the IPv6 or IP address of the TFTP server to be used. The address <ip> parameter is optional and if omitted the switch defaults to the TFTP server specified by the <code>tftp-server</code> command unless software download is to take place using a USB Mass Storage Device.
primary   secondary	This parameter determines if the image is the primary or secondary image.
image <image name>	This parameter is 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 newer than the currently running image.
diag <image name>	This parameter is the name of the diagnostic image to be downloaded from the TFTP server.
poe_module_image <image name>	This parameter is the name of the PoE module image to be downloaded from the TFTP server. This option is only available in 5000 Series switches that support Power Over Ethernet.

Variable	Value
no-reset	This parameter forces the switch to not reset after the software download is complete.
usb	In the 5530-24TFD or 5600 series switches, 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 and only one can be executed at a time.	

---

## Configuration files in ACLI

ACLI provides many options for working with configuration files. Through ACLI, configuration files can be displayed, stored, and retrieved.

For details, refer to the following:

- [Displaying the current configuration](#) on page 124
- [Storing the current configuration](#) on page 125
- [Restoring a system configuration](#) on page 127
- [Saving the current configuration](#) on page 128
- [Automatically downloading a configuration file with ACLI](#) on page 129

---

## Displaying the current configuration

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

### Procedure steps

1. Log on to the Privileged EXEC mode in the ACLI.
2. Display the current configuration parameters that differ from the default configuration by using the following command:

```
show running-config
```
3. Display all the current configuration parameters t by using the following command:

```
show running-config verbose
```
4. Display the current configuration for a specific application by using the following command:

```
show running-config module <value>
```

**! Important:**

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

## Variable definitions

Use the data in the following table to help you use the `show running-config [verbose] [module <value>]` command.

**Table 45: show running-config parameters**

Variable	Value
verbose	Displays all the configuration including defaults and nondefaults.
module <value>	Displays the 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]

## Storing the current configuration

Copy the running configuration to store the information. The `copy running-config` command copies the contents of the current configuration file to another location for storage. For all switches in the 5000 Series, the configuration file can be saved to a TFTP server. The Avaya Ethernet Routing Switch 5530-24TFD or 5600 Series switches also provide the ability to save the configuration file to a USB Mass Storage Device through the front panel USB drive.

## Procedure steps

1. Log on to the Privileged EXEC mode in the ACLI.
2. Copy the running configuration to the TFTP server by using the following command:

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

3. Copy the running configuration to the USB by using the following command:

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

## Variable definitions

The following table outlines the parameters of the `copy running-config [tftp address {<A.B.C.D>|<WORD>} | usb {[module <value>]| [verbose]}] filename <WORD>` command.

**Table 46: copy running-config parameters**

Variable	Value
address {<A.B.C.D> <WORD>}	Specifies the address of the TFTP server to be used: <ul style="list-style-type: none"> <li>• <i>A.B.C.D</i>—specifies the IP address.</li> <li>• <i>WORD</i>—specifies the IPv6 address.</li> </ul>
filename <WORD>	Specifies the name of the file that is created when the configuration is saved to the TFTP server or USB Mass Storage Device.
module <value>	Displays the 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] [I3] [I3-protocols] [lacc] [logging] [mac-security] [mlt] [nsna] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [ssh] [ssl] [stack] [stkmon] [stp] [vlacp] [vlan]
tftp	Copies all of the running configuration file to a specified file on the TFTP server.
verbose	Copies all the configuration, including defaults and non-defaults, to the USB.
usb	Copies all of the running configuration file to the USB.

---

## Restoring a system configuration

ACLI provides three commands for restoring a system configuration to a switch:

- [copy tftp config](#) on page 127
- [copy usb config](#) on page 127
- [copy tftp config unit](#) on page 128

### copy tftp config

Use this procedure to restore a configuration file stored on a TFTP server.

#### Procedure steps

Use the following command from Privileged EXEC mode:

```
copy tftp config address <A.B.C.D> filename <name>
```

#### Variable definitions

The following table outlines the parameters of the `copy tftp config` command.

**Table 47: copy tftp config command parameters**

Variable	Value
address <A.B.C.D>	The IP address of the TFTP server to be used.
filename <name>	The name of the file to be retrieved.

### copy usb config

Use this procedure to restore a configuration file stored on a USB Mass Storage Device.

#### Procedure steps

Use the following command from Privileged EXEC mode:

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

**\* Note:**

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

## copy tftp config unit

Use this procedure to enable the configuration of a switch in a stack to be copied to a stand-alone switch for the purpose of replacing units in a stack.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
copy tftp config unit address <A.B.C.D> filename <name> unit
<unit number>
```

### Variable definitions

The following table outlines the parameters of the `copy tftp config unit` command.

**Table 48: copy tftp config unit command parameters**

Variable	Value
address <A.B.C.D>	The IP address of the TFTP server to be used.
filename <name>	The name of the file to be used.
unit <unit number>	The number of the stack unit to be used.

---

## 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

Use this procedure to copy the current configuration to NVRAM.

### Procedure steps

Use the following command from Privileged EXEC mode:



```
write memory
```

## save config command

Use this procedure to copy the current configuration to NVRAM.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
save config
```

---

## Automatically downloading a configuration file with ACLI

Use this procedure to enable a script to be loaded and executed immediately as well as configure parameters to automatically download a configuration file when the switch or stack is booted.

### Procedure steps

Use the following command from Privileged EXEC mode:

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

**\* Note:**

The current switch settings relevant to this process can be viewed using the **show config-network** command. This command takes no parameters and must be executed in Privileged EXEC mode.

---

## Variable definitions

The following table outlines the parameters of the **configure network** command.

**Table 49: configure network command parameters**

Variable	Value
load-on-boot {disable   use- bootp   use- config}	Specifies the settings for automatically loading a configuration file when the system boots:

Variable	Value
	<ul style="list-style-type: none"> <li>• <code>disable</code> - disables the automatic loading of config file</li> <li>• <code>use-bootp</code> - specifies loading the ASCII configuration file at boot and using BootP to obtain values for the TFTP address and filename</li> <li>• <code>use-config</code> - specifies loading the ASCII configuration file at boot and using the locally configured values for the TFTP address and filename</li> </ul> <p><b>* Note:</b> If you omit this parameter, the system immediately downloads and runs the ASCII config file.</p>
<code>address &lt;A.B.C.D&gt;</code>	The IP address of the desired TFTP server.
<code>filename &lt;name&gt;</code>	The name of the configuration file to use in this process

---

## Terminal setup

Use this procedure to configure terminal settings.

These settings are transmit and receive speeds, terminal length, and terminal width.

### Procedure steps

Use the following command from User EXEC mode:

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

**\* Note:**

The `show terminal` command can be used at any time to display the current terminal settings. This command takes no parameters and is executed in the EXEC command mode.

---

## Variable definitions

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

**Table 50: terminal command parameters**

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

---

## Setting the default management interface

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

Use this procedure to change the default management interface.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
cmd-interface {cli | menu}
```

---

## Setting Telnet access

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

**\* Note:**

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

For details on viewing and changing the Telnet-allowed IP addresses and settings, refer to the following:

- [telnet-access command](#) on page 132
- [no telnet-access command](#) on page 133
- [default telnet-access command](#) on page 134

---

## telnet-access command

Use this procedure to configure the Telnet connection that is used to manage the switch

### Procedure steps

Use the following command from Global Configuration mode:

```
telnet-access [enable | disable] [login-timeout <1-10>] [retry
<1-100>] [inactive-timeout <0-60>] [logging {none | access |
failures | all}] [source-ip <1-50> <51-100> <A.B.C.D> <WORD>
[mask <A.B.C.D>]
```

### Variable definitions

The following table outlines the parameters of the `telnet-access` command.

**Table 51: telnet-access command parameters**

Variable	Value
enable   disable	Enables or disables Telnet connection.
login-timeout <1-10>	Specify in minutes the time to wait for Telnet and Console login before the connection closes. Enter an integer between 1 and 10.
retry <1-100>	Specify the number of times the user can enter an incorrect password before closing the connection. Enter an integer between 1 and 100.
inactive-timeout <0-60>	Specify in minutes the duration for an inactive session to be terminated.
logging {none   access   failures   all}	Specify the events whose details you want to store in the event log: none--Do not save access events in the log

Variable	Value
	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> <A.B.C.D> [mask <A.B.C.D>] [source-ip <51-100> <WORD>	Specify the source IP address from which connections are allowed. Enter the IP address in dotted-decimal notation. Mask specifies the subnet mask from which connections are allowed; enter IP mask in dotted-decimal notation. Specify the source IPv6 address and prefix from which to allow connections.

## no telnet-access command

Use this procedure to disable the Telnet connection.

### Procedure steps

Use the following command from Global Configuration mode:

- For an IPv4 address and mask pair:  
no telnet-access [source-ip [<1-50>]]
- For an IPv6 address and mask pair:  
no telnet-access [source-ip [<51-100>]]

## Variable definitions

The following table outlines the parameters of the **no telnet-access** command.

**Table 52: no telnet-access command parameters**

Variable	Value
source-ip [<1-50>] source- ip [<51-100>]	Disables the Telnet access. When you do not use the optional parameter, the source-ip list is cleared, meaning the first index is set to 0.0.0.0/0.0.0.0, the second to fiftieth indexes are set to 255.255.255.255/255.255.255.255, the fiftyfirst index is set to ::/0, and the fiftysecond to hundredth indexes are set to ffff:fff:fff:fff:fff:fff:fff:fff/128. When you specify a source-ip address, the specified pair is set to 255.255.255.255/255.255.255.255 for indexes between 1 and 50 and the specified pair is set to ffff:fff:fff:fff:fff:fff:fff:fff/128 for indexes between 51 and 100.

---

## default telnet-access command

Use this procedure to set the Telnet settings to the default values.

### Procedure steps

Use the following command from Global Configuration mode:

```
default telnet-access
```

---

## Setting boot parameters

The command outlined in this section is used for booting the switch or stack as well as setting boot parameters.

---

## boot command

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

### Procedure steps

Use the following command from Privileged EXEC mode:

```
boot [default] [partial default] [unit <unitno>]
```

**\* Note:**

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

## Variable definitions

The following table outlines the parameters of the `boot` command.

**Table 53: boot command parameters**

Variable	Value
default	Reboot the stack or switch and use the factory default configurations
partial-default	Reboot the stack or switch and use partial factory default configurations

Variable	Value
unit <unitno>	Unit number

---

## Defaulting to BootP-when-needed

The BootP default value is BootP-when-needed. This enables the switch to be booted and the system to automatically seek a BootP server for the IP address.

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

However, if the device does not have an assigned IP address and the BootP process times out, the BootP mode automatically changes to BootP disabled. But this change to BootP disabled is not stored, and the BootP reverts to the default value of BootP-when-needed after rebooting the device.

When the system is upgraded, the switch retains the previous BootP value. When the switch is defaulted 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 135
- [no ip bootp server command](#) on page 136
- [default ip bootp server command](#) on page 136

---

## ip bootp server command

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

This command is used to change the value of BootP from the default value, which is BootP-when-needed.

### Procedure steps


Use the following command from Global Configuration mode:

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

## Variable definitions

The following table outlines the parameters of the `ip bootp server` command.

**Table 54: ip bootp server command parameters**

Variable	Value
always   disable   last   needed	<p>Specifies when to use BootP:</p> <ul style="list-style-type: none"> <li>• always - Always use BootP</li> <li>• disable - never use BootP</li> <li>• last - use BootP or the last known address</li> <li>• needed - use BootP only when needed</li> </ul> <p> <b>Note:</b> The default value is to use BootP when needed.</p>

---

## no ip bootp server command

Use this procedure to disable the BootP server.

### Procedure steps

Use the following command from Global Configuration mode:

```
no ip bootp server
```

---

## default ip bootp server command

Use this procedure to use BootP when needed.

### Procedure steps

Use the following command from Global Configuration mode:

```
default ip bootp server
```

---

## shutdown command

The `shutdown` command provides a mechanism for safely shutting down a switch or stack without interfering with device processes or corrupting the software image. After this command



is issued, the configuration is saved, auto-save functionality is temporarily disabled, and configuration changes are not allowed until the switch or stack restarts. If the shutdown is cancelled, auto-save functionality returns to the state in which it was previously functioning.

Use this procedure to shut down a switch or stack.

### Procedure steps

Use the following command from Privileged EXEC mode:

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

---

## Variable definitions

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

**Table 55: shutdown command parameters**

Variable	Value
force	This parameter forces the shutdown without confirmation.
minutes-to-wait <1-60>	This parameter represents the number of minutes to wait before the shutdown occurs. If no value is specified, the default value of 10 minutes is used.
cancel	This parameter cancels a scheduled shutdown any time during the time period specified by the <b>minutes-to-wait</b> parameter.

---

## reload command

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

The reload command differs from the shutdown command in that the configuration is not explicitly saved after the command is issued. This means that any configuration changes must be explicitly saved before the switch or stack reloads.

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

Use this procedure to reload a switch or stack.

### Procedure steps

Use the following command from Privileged EXEC mode:

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

---

## Variable definitions

The following table outlines the parameters of the `reload` command.

**Table 56: reload command parameters**

Variable	Value
<code>force</code>	This parameter forces the reload without confirmation.
<code>minutes-to-wait</code> <code>&lt;1-60&gt;</code>	This parameter represents the number of minutes to wait before the reload occurs. If no value is specified, the default value of 10 minutes is used.
<code>cancel</code>	This parameter cancels a scheduled reload any time during the time period specified by the <code>minutes-to-wait</code> parameter.

---

## ACLI Help

Use this procedure to obtain help on the navigation and use of Command Line Interface (ACLI).

### Procedure steps

Use the following command:

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

 **Note:**

These commands are available in any command mode.

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 command modes available and ACLI commands used to access them.

---

## Clearing the default TFTP server with ACLI

Use this procedure to clear the TFTP server and reset it to 0.0.0.0.

## Procedure steps

The default TFTP server can be cleared from the switch and reset to 0.0.0.0 with the following two commands:

- `no tftp-server`

This command has no parameters and is executed from the Global Configuration command mode.

- `default tftp-server`

This command has no parameters and is executed from the Global Configuration command mode.

---

## Configuring a default TFTP server with ACLI

The switch processes that make use of a TFTP server often give the switch administrator the option of specifying the IP address of a TFTP server to be used. Instead of entering this address every time it is needed, a default IP address can be stored on the switch.

Use this procedure to specify a default TFTP server.

### Procedure steps

1. Use the following command from Privileged EXEC mode:

```
tftp-server [<ipv6_address> | <A.B.C.D>
```

2. To complete the command, replace either the `ipv6_address` or `<A.B.C.D>` with the IPv6 or IP address of the default TFTP server

---

## Displaying the default TFTP server with ACLI

Use this procedure to display the default TFTP server configured for the switch.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
show tftp-server
```

---

## Secure Transfer File Protocol configuration

This section describes Secure Transfer File Protocol (SFTP) configuration using the ACLI.

---

## Navigation

- [Uploading a config file to an SFTP server](#) on page 140
- [Downloading a config file to an SFTP server](#) on page 141
- [Enabling DSA authentication](#) on page 143
- [Disabling DSA authentication](#) on page 143
- [Enabling Password authentication](#) on page 143
- [Disabling Password authentication](#) on page 144
- [Setting the Transmission Control Protocol port](#) on page 144
- [Setting timeout](#) on page 145
- [Viewing SFTP](#) on page 145

---

## Uploading a config file to an SFTP server

Upload a config file to a SFTP server using SFTP protocol.

### Procedure steps

Use the following command from the Global Configuration mode:

```
copy config sftp address <A.B.C.D | WORD> filename <WORD>
[username <WORD> password <WORD>]
```

#### Important:

If you do not enter the username and password, and the default values are not available, you are prompted for these parameters if the password authentication is enable.

If the password authentication is disable and you enter the username and password, the password authentication changes from the inactive to active state.

### Variable definitions

Use the data in the following table to help you upload a config file.

**Table 57: copy config sftp address command parameters**

Variable	Value
address <A.B.C.D   WORD>	Specifies the address of the SFTP server:

Variable	Value
	<ul style="list-style-type: none"> <li>• <i>A.B.C.D</i> specifies the IP address.</li> <li>• <i>WORD</i> specifies the IPv6 address.</li> </ul>
filename <WORD>	Specifies the config file name.
password <WORD>	Specifies the password.
username <WORD>	Specifies the username.

## Downloading a config file to an SFTP server

Download a config file to a SFTP server using SFTP protocol.

### Procedure steps

Use the following command from the Global Configuration mode:

```
copy sftp config address <A.B.C.D | WORD> filename <WORD>
[username <WORD>][ password <WORD>]
```

#### Important:

If you do not enter the username and password, and the default values are not available, you are prompted for these parameters if the password authentication is enable.

If the password authentication is disable and you enter the username and password, the password authentication changes from the inactive to active state.

### Variable definitions

Use the data in the following table to help you upload a config file.

**Table 58: copy sftp config address command parameters**

Variable	Value
address <A.B.C.D   WORD>	Specifies the address of the SFTP server: <ul style="list-style-type: none"> <li>• <i>A.B.C.D</i> specifies the IP address.</li> <li>• <i>WORD</i> specifies the IPv6 address.</li> </ul>
filename <WORD>	Specifies the config file name.
password <WORD>	Specifies the password.
username <WORD>	Specifies the username.

## Host keys

This section describes how to configure host keys.

### Navigation

- [Generating a host key \(public and private\)](#) on page 142
- [Deleting the host keys \(public and private\)](#) on page 142
- [Uploading the public host key](#) on page 142

### Generating a host key (public and private)

Generate a host key to replace an old key in the NVRAM. The new key immediately becomes active and the DSA authentication state does not change.

#### Procedure steps

Use the following command from Global Configuration mode:

```
sshc dsa-host-key
```

### Deleting the host keys (public and private)

Delete the DSA host keys from the NVRAM. The DSA authentication state does not change.

#### Procedure steps

Use the following command from Global Configuration mode:

```
no sshc dsa-host-key
```

### Uploading the public host key

Upload the DSA public host key to an TFTP Server or an USB flash drive if available

#### Procedure steps

Use the following command from Global Configuration mode:

```
sshc upload-host-key address <A.B.C.D | WORD> filename <WORD>
```

OR

```
sshc upload-host-key usb filename <WORD> unit <#>
```

### Variable definitions

Use the data in the following table to help you upload the public host key.

**Table 59: sshc upload-host-key command parameters**

Variable	Value
address <A.B.C.D   WORD>	Specifies the address of the SFTP server: <ul style="list-style-type: none"> <li>• <i>A.B.C.D</i> specifies the IP address.</li> <li>• <i>WORD</i> specifies the IPv6 address.</li> </ul>
filename <WORD>	Specifies the config file name.
unit <#>	Specifies the unit number.
usb filename <WORD>	Specifies the USB key file.

---

## Enabling DSA authentication

Enable DSA authentication to generate DSA keys if they are not available.

### Procedure steps

Use the following command from Global Configuration mode:

```
sshc dsa-auth
```

---

## Disabling DSA authentication

Disable DSA authentication to generate DSA keys if they are not available.

### Procedure steps

Use the following command from Global Configuration mode:

```
no sshc dsa-auth
```

---

## Enabling Password authentication

Use this procedure to enable Password authentication.

## Procedure steps

Use the following command from Global Configuration mode:

```
sshc pass-auth
```

---

## Disabling Password authentication

Use this procedure to disable Password authentication.

## Procedure steps

Use the following command from Global Configuration mode:

```
no sshc pass-auth
```

---

## Setting the Transmission Control Protocol port

Use this procedure to set the Transmission Control Protocol (TCP) port.

## Procedure steps

Use the following command from Global Configuration mode:

```
sshc port TCP-port <portlist>
```

## Variable definitions

Use the data in the following table to help you set the TCP port.

**Table 60: sshc port TCP-port command parameters**

Variable	Value
portlist	Specifies the TCP port. The default port is 22.



---

## Setting timeout

Set the time expired used during a session.

### Procedure steps

Use the following command from Global Configuration mode:

```
sshc timeout <1-120>
```

### Variable definitions

Use the data in the following table to help you set the time expired parameter.

**Table 61: sshc timeout parameters**

Variable	Value
<1-120>	Specifies the time expired in the range of 1 to 120 seconds. The default is 60 seconds.

---

## Viewing SFTP

View the current SFTP configuration.

### Procedure steps

Use the following command from Global Configuration mode:

```
sshc show
```

### Job aid

The following table describes the fields for the `sshc show` command.

**Table 62: sshc show command**

Field	Description
Version	Specifies the current SSH version.

Field	Description
SFTP Server IP	Specifies the IP or IPv6 address.
Port	Specifies the port number.
The Remote Config File Name	Specifies the Filename.
DSA Authentication	Specifies if DSA authentication is enabled.
Password Authentication	Specifies if Password authentication is enabled
User Name (pw auth)	Specifies the use name.
Password (pw auth)	Specifies if
DSA Host Keys	
Key Gen In Process	Specifies whether key generation is in progress.

---

## Configuring daylight savings time with ACLI

Use the following procedure to configure the daylight savings time adjustment with ACLI:

1. Use the following command from Global Configuration mode:

```
configure
```

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]
```

---

## Variable definitions

The following table outlines the parameters of the `clock summer-time` command.

**Table 63: clock summer-time command parameters**

Variables	Value
date	Indicates that daylight savings time should start and end on the specified days every year.
day	Date to start daylight savings time.
month	Month to start daylight savings time.

Variables	Value
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

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.

```
clock summer-time BST date 28 Mar 2007 2:00 30 Aug 2007 15:00 +60
```

---

## Configuring default clock source with ACLI

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

### Procedure steps

Use the following command from Global Configuration mode:

```
clock source {rtp | sntp | sysUpTime}
```

**\* Note:**

Substitute {rtp | sntp | sysUpTime} with the clock source selection.

---

## Configuring local time zone with ACLI

SNTP uses Coordinated Universal Time (UTC) for all time synchronizations so it is not affected by different time zones. To have the switch report the time in your local time zone, you need to use the clock commands to set the local time zone.

You must enable SNTP before you set the time zone. If SNTP is not enabled, this command has no effect. If you enable SNTP and do not specify a time zone, UTC is shown by default.

Use this procedure to configure your switch for your local time zone.

### Procedure steps

1. Use the following command from Global Configuration mode:

```
configure
```

2. Enable sntp server.

3. Set clock time zone using the clock command.

```
clock time-zone zone hours [minutes]
```

---

## Variable definitions

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

**Table 64: clock time-zone command parameters**

Variable	Value
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.

---

## Configuring Dual Agent with ACLI

Use the following procedures to configure the Dual Agent feature with ACLI:

- [Enhanced download command](#) on page 148
- [Set the next boot Image](#) on page 150
- [Show agent images](#) on page 150

---

## Enhanced download command

You can update either active image or non-active image. Once the image download is done, the unit resets and restarts with the new image regardless of the value of the Next Boot image

indicator. In case of image download without reset, the new image in the flash will be the Next Boot image.

Use this procedure to specify the download target image.

### Procedure steps

Use the following command from Global Configuration mode:

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

### Variable definitions

The following table outlines the parameters of the `download` command.

**Table 65: download command parameters**

Variable	Value
ipv6_address	IPv6 IP address
a.b.c.d	IP address in dot notation.
primary   secondary	Choose which image to download.
image <image name>	Download the specified image.
image-if-newer <image name>	Only download the image if the version is newer than the installed version.
diag <image name>	Download the specified diagnostic image.
poe_module_image <image name>	Download the specified PoE module image.
no-reset	Do not reset the switch.
usb	Download the image from the USB drive.

**\* Note:**

Dual Agent supports the Ethernet Routing Switch 5510 NBUs through AAUR.

## Set the next boot image

You can use ACLI commands to change the next boot image of the device. Use the following procedures to change the next boot image:

- [toggle-next-boot-image](#) on page 150
- [boot secondary](#) on page 150

### toggle-next-boot-image

Use this procedure to toggle the next boot image.

#### Procedure steps

Use the following command from Global Configuration mode:

```
toggle-next-boot-image
```

**\* Note:**

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

### boot secondary

Use this procedure to use the secondary boot image.

#### Procedure steps

Use the following command from Global Configuration mode:

```
boot secondary
```

**\* Note:**

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

---

## Show agent images

You can use ACLI commands to list the following information about the agent images stored in flash memory:

- Primary image version
- Secondary image name
- Active image version

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

### Procedure steps

Use the following command from Global Configuration mode:

```
show boot image
```

---

## Configuring IPv6 with ACLI

Use the following procedures to configure IPv6:

- [Enabling IPv6 interface on the management VLAN](#) on page 152
- [Configuring IPv6 interface on the management VLAN](#) on page 152
- [Displaying the IPv6 interface information](#) on page 153
- [Displaying IPv6 interface addresses](#) on page 153
- [Configuring an IPv6 address for a switch or stack](#) on page 154
- [Displaying the IPv6 address for a switch or stack](#) on page 155
- [Configuring IPv6 management interface](#) on page 156
- [Disabling IPv6 globally](#) on page 157
- [Returning IPv6 to default settings](#) on page 157
- [Configuring IPv6 global properties](#) on page 158
- [Displaying the global IPv6 configuration](#) on page 158
- [Configuring an IPv6 default gateway for the switch or stack](#) on page 159
- [Displaying the IPv6 default gateway](#) on page 159
- [Configuring the IPv6 neighbor cache](#) on page 160
- [Displaying the IPv6 neighbor information](#) on page 160
- [Displaying IPv6 interface ICMP statistics](#) on page 161
- [Displaying IPv6 interface statistics](#) on page 162
- [Displaying IPv6 TCP statistics](#) on page 162
- [Displaying IPv6 TCP connections](#) on page 163
- [Displaying IPv6 TCP listeners](#) on page 163
- [Displaying IPv6 UDP statistics and endpoints](#) on page 163

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 this procedure to enable an IPv6 interface on the management VLAN.

### Procedure steps

1. Use the following command from Global Configuration mode:

```
interface vlan 1
```

2. Enter `ipv6 interface enable`.
3. Enter `exit` to return to the main menu.

Use this procedure to enable or disable `ipv6 admin status` and set `icmp error interval`:

### Procedure steps

1. Use the following command from Global Configuration mode:

```
[no] ipv6 enable [icmp error-interval <0-2147483647> | icmp  
unreach-msg]
```

2. Enter `exit` to return to the main menu.

## Variable definitions

The following table outlines the parameters for `ipv6 enable`:

**Table 66: IPv6 enable command parameteres**

Variable	Value
<code>enable</code>	Default admin status: enabled
<code>icmp error-interval &lt;0-2147483647&gt;</code>	Specifies the ICMP error interval. Values range from 0 to 2147483647 seconds.
<code>icmp unreach-msg</code>	Enables the IPv6 ICMP unreach message.

---

## Configuring IPv6 interface on the management VLAN

Use this procedure to assign an IPv6 address to a VLAN.

### Procedure steps

1. Use the following command from Global Configuration mode:



- ```
interface vlan 1
```
2. Enter `ipv6 interface enable`.
  3. Enter `exit` to return to the main menu.

---

## Displaying the IPv6 interface information

Use this procedure to display the IPv6 interface information.

### Procedure steps

Use the following command from Global Configuration mode:

```
show ipv6 interface
```

### Job aid

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

```
(config)#show ipv6 interface
-----
                                Interface Information
-----
IFINDX VLAN-ID MTU  PHYSICAL      ADMIN  OPER  RCHBLE  RETRAN  TYPE
                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  3000:0:0:0:0:0:99                      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.
```

Figure 19: show ipv6 interface

---

## Displaying IPv6 interface addresses

Use this procedure to view IPv6 interface addresses to learn the addresses.

Use the following command from User EXEC mode:

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

## Variable definitions

The following table outlines the parameters of the `show ipv6 address interface` command.

**Table 67: show ipv6 address interface command parameters**

| Variable      | Value                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------|
| <word 0-45>   | Specifies the IPv6 address length assigned to the management interface.                                     |
| vlan <1-4094> | Specifies the VLAN ID for which to display IPv6 interface address information. Values range from 1 to 4094. |

The following table shows the field descriptions for this command.

**Table 68: show ipv6 address interface command field descriptions**

| Field        | Value                                                                                                                                                                                                                                                                          |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv6 ADDRESS | Specifies the IPv6 destination address.                                                                                                                                                                                                                                        |
| VID/BID/TID  |                                                                                                                                                                                                                                                                                |
| 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: <ul style="list-style-type: none"> <li>• PREFERRED</li> <li>• DEPRECATED</li> <li>• INVALID</li> <li>• INACCESSIBLE</li> <li>• UNKNOWN</li> <li>• TENTATIVE</li> <li>• DUPLICATE</li> </ul> |

---

## Configuring an IPv6 address for a switch or stack

Use this procedure to configure and IPv6 address for a switch or stack.

## Procedure steps

Use the following command from Global Configuration mode:

```
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 outlines the parameters of the `ipv6 address` command.

**Table 69: IPv6 address command parameters**

| Variable                                | Value                                             |
|-----------------------------------------|---------------------------------------------------|
| <code>ipv6_address/prefix_length</code> | Specifies the IPv6 address and prefix length.     |
| <code>stack</code>                      | IPv6 address and prefix length of stack.          |
| <code>switch</code>                     | IPv6 address/prefix length of switch.             |
| <code>unit</code>                       | IPv6 address/prefix length of unit number: 1 to 8 |

---

## Displaying the IPv6 address for a switch or stack

Use this procedure to display the IPv6 address for a switch or stack.

### Procedure steps

Use the following command from Global Configuration mode:

```
show ipv6 address
```

Use this procedure to display all ipv6 interface addresses.

### Procedure steps

Use the following command from Global Configuration mode: `show ipv6 address interface`

## Job aid

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

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

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

**Figure 20: show ipv6 address interface**

## Configuring IPv6 management interface

Use this procedure to configure the IPv6 interface and create the VLAN IPv6 interface and set the parameter.

1. Use the following command from Global Configuration mode:

```
interface vlan <mgmt_vlan_id>
```

2. Enter `ipv6 interface [address <ipv6_address/prefix_length>]`

## Variable definitions

The following table outlines the parameters of the `ipv6 interface` command.

**Table 70: ipv6 interface command parameters**

| Variable                                    | Value                                                                                                        |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| address<br><ipv6_address/<br>prefix_length> | Address or prefix length.                                                                                    |
| name <1-255>                                | Name: integer from 1 to 255                                                                                  |
| link-local <WORD<br>0-19>                   | Interface identifier,                                                                                        |
| mtu <1280-9600>                             | Default status: MTU 1280                                                                                     |
| reachable-time<br><0-3600000>               | Time in milliseconds neighbor is considered reachable after a reachable confirmation message. Default: 30000 |
| retransmit-timer<br><0-3600000>             | Time in milliseconds between retransmissions of neighbor solicitation messages to a neighbor. Default: 1000  |

---

## Disabling IPv6 globally

Use this procedure to disable IPv6 globally.

### Procedure steps

Use the following command from Global Configuration mode:

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

**\* Note:**

If you do not specify a parameter, you can use the `no ipv6 interface` to delete an IPv6 interface.

### Variable definitions

The following table outlines the parameters for the `no ipv6 interface` command.

**Table 71: no ipv6 interface command parameters**

| Variable | Value                                                              |
|----------|--------------------------------------------------------------------|
| address  | Delete an IPv6 address.                                            |
| all      | Disable interface administrative status or delete an IPv6 address. |
| enable   | Disable interface administrative status.                           |

---

## Returning IPv6 to default settings

Use this procedure to return an IPv6 interface or address to the default settings.

### Procedure steps

Use the following command from Global Configuration mode:

```
default ipv6 interface [all | enable | link-local | mtu |  
reachable-time | retransmit-timer】
```

### Variable definitions

The following table outlines the parameters for the `default ipv6 interface` command.

**Table 72: default ipv6 interface command parameters**

| Variable         | Value                                                              |
|------------------|--------------------------------------------------------------------|
| all              | Disable interface administrative status or delete an IPv6 address. |
| enable           | Disable interface administrative status.                           |
| link-local       | Default identifier.                                                |
| mtu              | Default MTU.                                                       |
| reachable-time   | Default reachable time.                                            |
| retransmit-timer | Default retransmit timer.                                          |

---

## Configuring IPv6 global properties

Use this procedure to configure the IPv6 global properties.

### Procedure steps

Use the following command from Global Configuration mode:

```
ipv6 [enable | icmp <error-interval / unreachable>]
```

### Variable definitions

The following table outlines the parameters for the `ipv6` command.

**Table 73: ipv6 command parameters**

| Variable | Value                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enable   | Enable the IPv6 global administrative status.                                                                                                                                                |
| icmp     | Set the IPv6 ICMP parameters. <ul style="list-style-type: none"> <li>• error-interval: Set the IPv6 ICMP error interval.</li> <li>• unreachable: Enable the IPv6 ICMP unreachable</li> </ul> |

---

## Displaying the global IPv6 configuration

Use this procedure to display the global IPv6 configuration.

## Procedure steps

Use the following command from Global Configuration mode:

```
show ipv6 global
```

## Job aid

The following table describes the `show ipv6 global` command results.

**Table 74: show ipv6 global command results**

| Field                  | Default setting |
|------------------------|-----------------|
| forwarding             | disabled        |
| default-hop-cnt        | 30              |
| number-of-interfaces   | 1               |
| admin-status           | enabled         |
| icmp-error-interval    | 1000            |
| icmp-redirect-msg      | disabled        |
| icmp-unreach-msg       | disabled        |
| multicast-admin-status | disabled        |

---

## Configuring an IPv6 default gateway for the switch or stack

Use this procedure to configure an IPv6 default gateway for the switch or stack.

### Procedure steps

1. Use the following command from Global Configuration mode:
 

```
ipv6 default-gateway <ipv6_gateway_address>
```
2. Enter `no ipv6 default-gateway` to disable a default gateway.

---

## Displaying the IPv6 default gateway

Use this procedure to display the IPv6 address for the default gateway.

### Procedure steps

Use the following command from Global Configuration mode:

```
show ipv6 default-gateway
```

---

## Configuring the IPv6 neighbor cache

Use this procedure to add or remove a static neighbor cache entry.

### Procedure steps

1. Use the following command from Global Configuration mode to add a static neighbor cache:

```
ipv6 neighbor <ipv6_address> [port <port/slot>] [mac <H.H.H>]
```

2. Use the following command from Global Configuration mode to remove a static neighbor cache entry:

```
no ipv6 neighbor <ipv6_address> [port <port/slot>] [mac  
<H.H.H>]
```

---

## Displaying the IPv6 neighbor information

Use this command to display IPv6 neighbor information.

### Procedure steps

Use the following command from Global Configuration mode:

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

## Job aid

The following figure shows the output of the `show ipv6 neighbor` command.



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

Figure 21: show ipv6 neighbor

---

## Displaying IPv6 interface ICMP statistics

Use this procedure to display IPv6 interface ICMP statistics.

Use the following command from Global Configuration mode:

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

### Job aid

The following figure shows a sample of the results from the `show ipv6 interface icmpstatistics` command.

```
(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
IcmpInEchos : 0
IcmpInEchoReplies : 0
<truncated>
```

Figure 22: show ipv6 interface icmpstatistics

---

## Displaying IPv6 interface statistics

Use this procedure to display IPv6 TCP statistics.

Use the following command from Global Configuration mode:

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

### Job aid

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

```
(config)#show ipv6 interface statistics
-----
                                Interface Stats
-----
If stats for IfIndex = 10001

InReceives: 0
InHdrErrors: 0
InTooBigErrors : 0
InNoRoutes : 0
InAddrErrors : 0
InUnknownProtes : 0
InTruncatedPkts : 0
InDiscards : 0
InDelivers : 20
<truncated>
```

Figure 23: show ipv6 interface statistics

---

## Displaying IPv6 TCP statistics

Use this procedure to display IPv6 TCP statistics.

### Procedure steps

Use the following command from Global Configuration mode:

```
show ipv6 tcp
```

### Job aid

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

```
(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
```

Figure 24: show ipv6 tcp

---

## Displaying IPv6 TCP connections

Use this procedure to display IPv6 TCP connections.

### Procedure steps

Use the following command from Global Configuration mode:

```
show ipv6 tcp connections [<WORD 0-128>] [<portList>] [<WORD
0-128>]
```

---

## Displaying IPv6 TCP listeners

Use this procedure to display IPv6 TCP listeners.

### Procedure steps

Use the following command from Global Configuration mode:

```
show ipv6 tcp listener
```

---

## Displaying IPv6 UDP statistics and endpoints

Use this procedure to display IPv6 UDP statistics and endpoints.

### Procedure steps

1. Use the following command from Global Configuration mode to show UDP statistics:

```
show ipv6 udp
```

2. Use the following command from Global Configuration mode to show UDP endpoints:

```
show ipv6 udp endpoints
```

---

## Configuring LLDP with ACLI

You can enable and configure LLDP with ACLI. For more information about LLDP, see [Link Layer Discover Protocol \(IEEE 802.1ab\) Overview](#) on page 65. This section covers the following commands:

- [lldp command](#) on page 165
- [lldp port command](#) on page 165
- [lldp tx-tlv command](#) on page 166
- [lldp tx-tlv dot1 command](#) on page 167
- [lldp tx-tlv dot3 command](#) on page 167
- [lldp tx-tlv med command](#) on page 168
- [lldp location-identification coordinate-base command](#) on page 169
- [lldp location-identification civic-address command](#) on page 170
- [lldp location-identification ecs-elin command](#) on page 171
- [default lldp command](#) on page 172
- [default lldp port command](#) on page 172
- [default lldp tx-tlv command](#) on page 173
- [default lldp tx-tlv dot1 command](#) on page 174
- [default lldp tx-tlv dot3 command](#) on page 174
- [default lldp tx-tlv med command](#) on page 175
- [no lldp port command](#) on page 176
- [no lldp tx-tlv command](#) on page 176
- [no lldp tx-tlv dot1 command](#) on page 176
- [no lldp tx-tlv dot3 command](#) on page 177
- [no lldp tx-tlv med command](#) on page 177
- [show lldp command](#) on page 177
- [show lldp port command](#) on page 179
- [Configuring LLDP MED policies for switch ports](#) on page 180

- [Setting lldp med-network-policies to the default values](#) on page 181
- [Disabling LLDP MED policies for switch ports](#) on page 181
- [Viewing lldp med-network-policies](#) on page 182
- [Configuring LLDP](#) on page 183

---

## Ildp command

Use this procedure to set the LLDP transmission parameters.

### Procedure steps

Use the following command from Global Configuration mode:

```
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>]
```

## Variable definitions

The following table outlines the parameters of the `lldp` command.

**Table 75: Ildp command parameters**

| Variable                           | Value                                                                                          |
|------------------------------------|------------------------------------------------------------------------------------------------|
| tx-interval<br><5-32768>           | sets the interval between successive transmission cycles                                       |
| tx-hold-<br>multiplier <2-10>      | sets the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV |
| reinit-delay<br><1-10>             | sets the delay for the reinitialization attempt if the adminStatus is disabled                 |
| tx-delay <1-8192>                  | sets the minimum delay between successive LLDP frame transmissions                             |
| notification-<br>interval <5-3600> | sets the interval between successive transmissions of LLDP notifications                       |
| med-fast-start<br><1-10>           | sets the MED Fast Start repeat count value                                                     |

---

## Ildp port command

Use this procedure to set the LLDP port parameters.

## Procedure steps

Use the following command from Interface Configuration mode:

```
lldp port <portlist> [config notification] [status {rxOnly |
txAndRx | txOnly}]
```

## Variable definitions

The following table outlines the parameters of the `lldp port` command.

**Table 76: lldp port command parameters**

| Variable                           | Value                                                                                                                                                                     |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| port <portlist>                    | specifies the ports affected by the command                                                                                                                               |
| config notification                | enables notification when new neighbor information is stored or when existing information is removed                                                                      |
| status {rxOnly   txAndRx   txOnly} | sets the LLDP transmit and receive status on the ports rxonly: enables LLDP receive only. txAndRx: enables LLDP transmit and receive. txOnly: enables LLDP transmit only. |

---

## lldp tx-tlv command

Use this procedure to set the optional Management TLVs to be included in the transmitted LLDPUs.

### Procedure steps

Use the following command from Interface Configuration mode:

```
lldp tx-tlv [port <portlist>] [local-mgmt-addr] [port-desc]
[sys-cap] [sys-desc] [sys-name]
```

## Variable definitions

The following table outlines the parameters of the `lldp tx-tlv` command.

**Table 77: lldp tx-tlv command variables**

| Variables       | Value                                        |
|-----------------|----------------------------------------------|
| local-mgmt-addr | Specifies the local management address TLV.  |
| port <portlist> | Specifies the ports affected by the command. |
| port-desc       | Specifies the port description TLV.          |

| Variables             | Value                                  |
|-----------------------|----------------------------------------|
| <code>sys-cap</code>  | Specifies the system capabilities TLV. |
| <code>sys-desc</code> | Specifies the system description TLV.  |
| <code>sys-name</code> | Specifies the system name TLV.         |

---

## lldp tx-tlv dot1 command

Use this procedure to set the optional IEEE 802.1 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

### Procedure steps

Use the following command from Interface Configuration mode:

```
lldp tx-tlv [port <portlist>] dot1 [port-protocol-vlan-id
<vlanlist>] [port-vlan-id] {protocol-identity [EAP] [LLDP]
[STP]} [vlan-name <vlanlist>]
```

## Variable definitions

The following table outlines the parameters of the `lldp tx-tlv dot1` command.

**Table 78: lldp tx-tlv dot1 command parameters**

| Variable                                          | Value                                       |
|---------------------------------------------------|---------------------------------------------|
| <code>port &lt;portlist&gt;</code>                | specifies the ports affected by the command |
| <code>port-vlan-id</code>                         | Port VLAN ID TLV                            |
| <code>vlan-name</code>                            | VLAN Name TLV                               |
| <code>port-protocol-vlan-id</code>                | Port and Protocol VLAN ID TLV               |
| <code>protocol-identity [EAP] [LLDP] [STP]</code> | Protocol Identity TLV                       |

---

## lldp tx-tlv dot3 command

Use this procedure to set the optional IEEE 802.3 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

## Procedure steps

Use the following command from Interface Configuration mode:

```
lldp tx-tlv [port <portlist>] dot3 [link-aggregation] [mac-phy-
config-status] [maximum-frame-size] [mdi-power-support]
```

## Variable definitions

The following table outlines the parameters of the `lldp tx-tlv dot3` command.

**Table 79: lldp tx-tlv dot3 command parameters**

| Variable              | Value                                       |
|-----------------------|---------------------------------------------|
| port <portlist>       | specifies the ports affected by the command |
| mac-phy-config-status | MAC/Phy Configuration/Status TLV            |
| mdi-power-support     | Power Via MDI TLV                           |
| link-aggregation      | Link Aggregation TLV                        |
| maximum-frame-size    | Maximum Frame Size TLV                      |

---

## lldp tx-tlv med command

Use this procedure to set the optional organizationally-specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

### Procedure steps

Use the following command from Interface Configuration mode:

```
lldp tx-tlv [port <portlist>] med [extendedPSE] [inventory]
[location] [med-capabilities] [network-policy]
```

## Variable definitions

The following table outlines the parameters of the `lldp tx-tlv med` command.

**Table 80: lldp tx-tlv med command parameters**

| Variable        | Value                                       |
|-----------------|---------------------------------------------|
| port <portlist> | specifies the ports affected by the command |



| Variable         | Value                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------|
| med-capabilities | MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted) |
| extendedPSE      | Extended PSE TLV                                                                              |
| inventory        | Inventory TLVs                                                                                |
| location         | Location Identification TLV                                                                   |
| network-policy   | Network Policy TLV                                                                            |

## lldp location-identification coordinate-base command

Use this procedure to set the coordinate-base parameters for LLDP location identification information.

### Procedure steps

Use the following command from Interface Configuration mode:

```
lldp location-identification coordinate-base [altitude] [datum]
[latitude] [longitude]
```

## Variable definitions

The following table outlines the parameters of the `lldp location-identification coordinate-base` command.

**Table 81: lldp location-identification coordinate-base command parameters**

| Variable                                                            | Value                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| altitude [ +   - ]<br>[0-4194303.fracti<br>on] [meters  <br>floors] | Altitude, in meters or floors.                                                                                                                                                                                                                                                                                                   |
| datum [NAD83/MLLW<br>  NAD83/NAVD88  <br>WGS84]                     | Reference datum<br>The valid options are: <ul style="list-style-type: none"> <li>• NAD83/MLLW: North American Datum 1983, Mean Lower Low Water</li> <li>• NAD83/NAVD88: North American Datum 1983, North American Vertical Datum of 1988</li> <li>• WGS84: World Geodesic System 1984, Prime Meridian Name: Greenwich</li> </ul> |

| Variable                                 | Value                                                     |
|------------------------------------------|-----------------------------------------------------------|
| latitude<br>[0-90.00] [NORTH<br>  SOUTH] | Latitude in degrees, and relative to the equator.         |
| longitude<br>[0-180.00] [EAST<br>  WEST] | Longitude in degrees, and relative to the prime meridian. |

---

## lldp location-identification civic-address command

Use this procedure to set the LLDP civic address parameters.

### Procedure steps

Use the following command from Interface Configuration mode:

```
lldp location-identification civic-address country-code
[additional-code] [additional-information] [apartment] [block]
[building] [city] [city-district ] [county] [floor] [house-
number] [house-number-suffix] [landmark] [leading-street-
direction] [name] [p.o.box] [place-type] [postal-community-
name] [postal/zip-code] [room-number] [state] [street] [street-
suffix] [trailing-street-suffix]
```

### Variable definitions

The following table outlines the parameters of the `lldp location-identification civic-address` command.

**Table 82: lldp location-identification civic-address command parameters**

| Variable               | Value                              |
|------------------------|------------------------------------|
| additional-code        | Additional code                    |
| additional-information | Additional location information    |
| apartment              | Unit (apartment, suite)            |
| block                  | Neighborhood, block                |
| building               | Building (structure)               |
| city                   | City, township, shi (JP)           |
| city-district          | City division, city district, ward |

| Variable                 | Value                                         |
|--------------------------|-----------------------------------------------|
| country-code             | Country code value (2 capital letters)        |
| county                   | County, parish, gun (JP), district (IN)       |
| floor                    | Floor                                         |
| house-number             | House number                                  |
| house-number-suffix      | House number suffix                           |
| landmark                 | Landmark or vanity address                    |
| leading-street-direction | Leading street direction                      |
| name                     | Residence and office occupant                 |
| p.o.box                  | Post office box                               |
| place-type               | Office                                        |
| postal-community-name    | Postal community name                         |
| postal/zip-code          | Postal/Zip code                               |
| room-number              | Room number                                   |
| state                    | National subdivisions (state, canton, region) |
| street                   | Street                                        |
| street-suffix            | Street suffix                                 |
| trailing-street-suffix   | Trailing street suffix                        |

---

## lldp location-identification ecs-elin command

Use this procedure to set the LLDP emergency call service - emergency location identification number (ECS-ELIN).

### Procedure steps

Use the following command from Interface Configuration mode:

```
lldp location-identification ecs-elin <ecs-elin>
```

**\* Note:**

<ecs-elin> specifies a 10 to 25 digit numerical string.

---

## default lldp command

Use this procedure to set the LLDP transmission parameters to their default values.

### Procedure steps

Use the following command from Global Configuration mode:

```
default lldp [tx-interval ] [tx-hold-multiplier ] [reinit-
delay] [tx-delay] [notification-interval] [med-fast-start]
```

**\* Note:**

If no parameters are specified, the `default lldp` sets all parameters to their default parameters.

## Variable definitions

The following table outlines the parameters of the `default lldp` command.

**Table 83: default lldp command parameters**

| Variable              | Value                                                               |
|-----------------------|---------------------------------------------------------------------|
| tx-interval           | sets the retransmit interval to the default value (30)              |
| tx-hold-multiplier    | sets the transmission multiplier to the default value (4)           |
| reinit-delay          | sets the reinitialize delay to the default value (2)                |
| tx-delay              | sets the transmission delay to the default value (2)                |
| notification-interval | sets the notification interval to the default value (5)             |
| med-fast-start        | sets the MED Fast Start repeat count value to the default value (4) |

---

## default lldp port command

Use this procedure to set the port parameters to their default values.

## Procedure steps

Use the following command from Interface Configuration mode:

```
default lldp port <portlist> [config notification] [status]
```

## Variable definitions

The following table outlines the parameters of the `default lldp port` command.

**Table 84: default lldp port command parameters**

| Variable            | Value                                                                    |
|---------------------|--------------------------------------------------------------------------|
| port <portlist>     | specifies the ports affected by the command                              |
| config notification | sets the config notification to its default value (disabled)             |
| status              | sets the LLDP transmit and receive status to the default value (txAndRx) |

---

## default lldp tx-tlv command

Use this procedure to set the LLDP Management TLVs to their default values.

### Procedure steps

Use the following command from Interface Configuration mode:

```
default lldp tx-tlv [port <portlist>][port-desc] [sys-name]
[sys-desc] [sys-cap] [local-mgmt-addr]
```

## Variable definitions

The following table outlines the parameters of the `default lldp tx-tlv` command.

**Table 85: default lldp tx-tlv command parameters**

| Variable        | Value                                                          |
|-----------------|----------------------------------------------------------------|
| port <portlist> | specifies the ports affected by the command                    |
| port-desc       | Port description TLV (default value is false: not included)    |
| sys-name        | System name TLV (default value is false: not included)         |
| sys-desc        | System description TLV (default value is false: not included)  |
| sys-cap         | System capabilities TLV (default value is false: not included) |

| Variable        | Value                                                               |
|-----------------|---------------------------------------------------------------------|
| local-mgmt-addr | Local management address TLV (default value is false: not included) |

---

## default lldp tx-tlv dot1 command

Use this procedure to set the optional IEEE 802.1 organizationally-specific TLVs to their default values.

### Procedure steps

Use the following command from Interface Configuration mode:

```
default lldp tx-tlv [port <portlist>] dot1 [port-vlan-id]
[vlan-name ] [port-protocol-vlan-id] [protocol-identity [EAP]
[LLDP] [STP] ]
```

## Variable definitions

The following table outlines the parameters of the `default lldp tx-tlv dot1` command.

**Table 86: default lldp tx-tlv dot1 command parameters**

| Variable                                   | Value                                                   |
|--------------------------------------------|---------------------------------------------------------|
| port <portlist>                            | specifies the ports affected by the command             |
| port-vlan-id                               | Port VLAN ID TLV (default value is false: not included) |
| vlan-name                                  | VLAN Name TLV (default value is none)                   |
| port-protocol-vlan-id                      | Port and Protocol VLAN ID TLV (default value is none)   |
| protocol-identity<br>[EAP] [LLDP]<br>[STP] | Protocol Identity TLV (default value is none)           |

---

## default lldp tx-tlv dot3 command

Use this procedure to set the optional IEEE 802.3 organizationally-specific TLVs to their default values.

## Procedure steps

Use the following command from Interface Configuration mode:

```
default lldp tx-tlv [port <portlist>] dot3 [mac-phy-config-
status] [mdi-power-support] [link-aggregation][maximum-frame-
size]
```

## Variable definitions

The following table outlines the parameters of the `default lldp tx-tlv dot3` command.

**Table 87: default lldp tx-tlv dot3 command parameters**

| Variable              | Value                                                                   |
|-----------------------|-------------------------------------------------------------------------|
| port <portlist>       | specifies the ports affected by the command                             |
| mac-phy-config-status | MAC/Phy Configuration/Status TLV (default value is false: not included) |
| mdi-power-support     | Power Via MDI TLV (default value is false: not included)                |
| link-aggregation      | Link Aggregation TLV (default value is false: not included)             |
| maximum-frame-size    | Maximum Frame Size TLV (default value is false: not included)           |

---

## default lldp tx-tlv med command

Use this procedure to set the optional organizationally-specific TLVs for MED devices to their default values.

### Procedure steps

Use the following command from Interface Configuration mode:

```
default lldp tx-tlv [port <portlist>] med [med-capabilities]
[extendedPSE] [inventory] [location] [network-policy]
```

## Variable definitions

The following table outlines the parameters of the `default lldp tx-tlv med` command.

**Table 88: default lldp tx-tlv med command parameters**

| Variable         | Value                                                              |
|------------------|--------------------------------------------------------------------|
| port <portlist>  | specifies the ports affected by the command                        |
| med-capabilities | MED Capabilities TLV (default value is false: not included)        |
| extendedPSE      | Extended PSE TLV (default value is false: not included)            |
| inventory        | Inventory TLVs (default value is false: not included)              |
| location         | Location Identification TLV (default value is false: not included) |
| network-policy   | Network Policy TLV (default value is false: not included)          |

---

## no lldp port command

Use this procedure to disable LLDP features on the port.

### Procedure steps

Use the following command from Interface Configuration mode:

```
no lldp [port <portlist>] [config notification] [status]
```

---

## no lldp tx-tlv command

Use this procedure to specify the optional Management TLVs not to include in the transmitted LLDPDUs.

### Procedure steps

Use the following command from Interface Configuration mode:

```
no lldp tx-tlv [port <portlist>] [port-desc] [sys-name] [sys-  
desc] [sys-cap] [local-mgmt-addr]
```

---

## no lldp tx-tlv dot1 command

Use this procedure to specify the optional IEEE 802.1 TLVs not to include in the transmitted LLDPDUs.

### Procedure steps

Use the following command from Interface Configuration mode:



```
no lldp tx-tlv [port <portlist>] dot1 [port-vlan-id] [vlan-
name] [port-protocol-vlan-id] [protocol-identity [EAP] [LLDP]
[STP] ]
```

---

## no lldp tx-tlv dot3 command

Use this procedure to specify the optional IEEE 802.3 TLVs not to include in the transmitted LLDPDUs.

### Procedure steps

Use the following command from Interface Configuration mode:

```
no lldp tx-tlv [port <portlist>] dot3 [mac-phy-config-status]
[mdi-power-support] [link-aggregation][maximum-frame-size]
```

---

## no lldp tx-tlv med command

Use this procedure to specify the optional Management TLVs not to include in the transmitted LLDPDUs.

### Procedure steps

Use the following command from Interface Configuration mode:

```
no lldp tx-tlv [port <portlist>] med [med-capabilities]
[extendedPSE] [inventory] [location] [network-policy]
```

---

## show lldp command

Use this procedure to display the LLDP parameters.

### Procedure steps

Use the following command from User EXEC mode:

```
show lldp [local-sys-data {dot1 | dot3 | med | detail}] [mgmt-
sys-data] [rx-stats] [tx-stats] [stats] [pdu-tlv-size] [tx-tlv
{dot1 | dot3 | med }] [neighbor { dot1 [vlan-names | protocol-
id] } | [dot3] | { med [capabilities] [network-policy]
[location] [extended-power] [inventory] } | [detail] ]
[neighbor-mgmt-addr]
```

## Variable definitions

The following table outlines the parameters of the **show lldp** command.

**Table 89: show lldp command parameters**

| Variable                                                                                                                                                      | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>local-sys-data {dot1   dot3   med   detail}</pre>                                                                                                        | <p>Displays the organizationally-specific TLV properties on the local switch:</p> <ul style="list-style-type: none"> <li>• dot1: displays the 802.1 TLV properties</li> <li>• dot3: displays the 802.3 TLV properties</li> <li>• med: displays the MED TLV properties</li> <li>• detail: displays all organizationally specific TLV properties</li> </ul> <p>To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.</p>                                                                                                                                                               |
| mgmt-sys-data                                                                                                                                                 | Displays the local management system data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| rx-stats                                                                                                                                                      | Displays the LLDP receive statistics for the local system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| tx-stats                                                                                                                                                      | Displays the LLDP transmit statistics for the local system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| stats                                                                                                                                                         | Displays the LLDP table statistics for the remote system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| pdu-tlv-size                                                                                                                                                  | Displays the different TLV sizes and the number of TLVs in an LLDPDU.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <pre>tx-tlv {dot1   dot3   med }</pre>                                                                                                                        | <p>Displays which TLVs are transmitted from the local switch in LLDPDUs:</p> <ul style="list-style-type: none"> <li>• dot1: displays status for 802.1 TLVs</li> <li>• dot3: displays status for 802.3 TLVs</li> <li>• med: displays status for MED TLVs</li> </ul> <p>To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.</p>                                                                                                                                                                                                                                                     |
| <pre>neighbor { dot1 [vlan-names   protocol-id] }   [dot3]   { med [capabilities] [network-policy] [location] [extended-power] [inventory] }   [detail]</pre> | <p>Displays the neighbor TLVs:</p> <ul style="list-style-type: none"> <li>• dot1: displays 802.1 TLVs: <ul style="list-style-type: none"> <li>- vlan-names: VLAN Name TLV</li> <li>- protocol-id: Protocol Identity TLV</li> </ul> </li> <li>• dot3: displays 802.3 TLVs</li> <li>• med: displays MED TLVs: <ul style="list-style-type: none"> <li>- capabilities: Capabilities TLV</li> <li>- network-policy: Network Policy Discovery TLV</li> <li>- location: Location Identification TLV</li> <li>- extended-power: Extended Power-via-MDI TLV</li> <li>- inventory: Inventory TLVs</li> </ul> </li> <li>• detail: displays all TLVs</li> </ul> |

| Variable             | Value                                          |
|----------------------|------------------------------------------------|
| [neighbor-mgmt-addr] | Displays the LLDP neighbor management address. |

## show lldp port command

Use this procedure to display the LLDP port parameters.

### Procedure steps

Use the following command from User EXEC mode:

```
show lldp port <portlist> [rx-stats] [tx-stats] [pdu-tlv-size]
[tx-tlv {dot1 | dot3 | med}] [neighbor {dot1 [vlan-names |
protocol-id] } | [dot3] | {med [capabilities] [network-policy]
[location] [extended-power] [inventory]} | [detail] ]]
[neighbor-mgmt-addr]
```

## Variable definitions

The following table outlines the parameters of the `show lldp port` command.

**Table 90: show lldp port command parameters**

| Variable                                                                     | Value                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rx-stats                                                                     | Displays the LLDP receive statistics for the local port.                                                                                                                                                                                                                                                                                                                                      |
| tx-stats                                                                     | Displays the LLDP transmit statistics for the local port.                                                                                                                                                                                                                                                                                                                                     |
| pdu-tlv-size                                                                 | Displays the different TLV sizes and the number of TLVs in an LLDPDU.                                                                                                                                                                                                                                                                                                                         |
| tx-tlv {dot1   dot3   med }                                                  | <p>Displays which TLVs are transmitted from the local port in LLDPDUs:</p> <ul style="list-style-type: none"> <li>• dot1: displays status for 802.1 TLVs</li> <li>• dot3: displays status for 802.3 TLVs</li> <li>• med: displays status for MED TLVs</li> </ul> <p>To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.</p> |
| neighbor { dot1 [vlan-names   protocol-id] }   [dot3]   { med [capabilities] | <p>Displays the port neighbor TLVs:</p> <ul style="list-style-type: none"> <li>• dot1: displays 802.1 TLVs: <ul style="list-style-type: none"> <li>- vlan-names: VLAN Name TLV</li> <li>- protocol-id: Protocol Identity TLV</li> </ul> </li> <li>• dot3: displays 802.3 TLVs</li> </ul>                                                                                                      |

| Variable                                                                          | Value                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [network-policy]<br>[location]<br>[extended-power]<br>[inventory] }  <br>[detail] | <ul style="list-style-type: none"> <li>• med: displays MED TLVs: <ul style="list-style-type: none"> <li>- capabilities: Capabilities TLV</li> <li>- network-policy: Network Policy Discovery TLV</li> <li>- location: Location Identification TLV</li> <li>- extended-power: Extended Power-via-MDI TLV</li> <li>- inventory: Inventory TLVs</li> </ul> </li> <li>• detail: displays all TLVs.</li> </ul> |
| [neighbor-mgmt-addr]                                                              | Displays the port neighbor LLDP management address.                                                                                                                                                                                                                                                                                                                                                       |

## Configuring LLDP MED policies for switch ports

Use the following procedure to configure LLDP Media Endpoint Devices (MED) policies.

### Procedure steps

Use the following command from the Interface Configuration mode:

```
lldp med-network-policies [port <portList>] {voice|voice-
signaling} [dscp <0-63>] [priority <0-7>] [tagging {tagged|
untagged}] [vlan-id <1-4094>]
```

### Variable definitions

The following table outlines the parameters of the `lldp med-network-policies` command.

**Table 91: lldp med-network-policies**

| Variable        | Value                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| port <portlist> | Specifies the port or ports on which to configure LLDP MED policies.                                                                                                                            |
| voice           | Specifies voice network policy.                                                                                                                                                                 |
| 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. |
| 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.                                                                            |

| Variable                    | Value                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tagging {tagged   untagged} | <p>Specifies the type of VLAN tagging to apply on the selected switch port or ports.</p> <ul style="list-style-type: none"> <li>• tagged—uses a tagged VLAN</li> <li>• untagged—uses an untagged VLAN or does not support port-based VLANs.</li> </ul> <p>If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.</p> |
| vlan-id <1-4094>            | <p>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.</p>                                                                                                                          |

## Setting lldp med-network-policies to the default values

Use this procedure to return lldp med-network-policies to the default values.

### Procedure steps

Use the following command from the Interface Configuration mode:

```
default lldp med-network-policies [port <portList>] {voice|
voice-signaling}
```

Variable definitions

The following table outlines the parameters of the `default lldp med-network-policies` command.

**Table 92: default lldp med-network-policies parameters**

| Variable        | Value                                                                        |
|-----------------|------------------------------------------------------------------------------|
| port <portlist> | Specifies the port or ports on which to configure default LLDP MED policies. |
| voice           | Specifies the default voice network policy.                                  |
| voice-signaling | Specifies the default voice signalling network policy.                       |

## Disabling LLDP MED policies for switch ports

Use this procedure to disable LLDP MED policies for switch ports.

## Procedure steps

Use the following command from the Interface Configuration mode:

```
no lldp med-network-policies [port <portlist>] {voice|voice-signaling}
```

### Variable definitions

The following table outlines the parameters of the `no lldp med-network-policies` command.

**Table 93: no lldp med-network-policies parameters**

| 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.          |

---

## Viewing lldp med-network-policies

Use this procedure to display LLDP MED policy information for switch ports.

### Procedure steps

Use the following command from the Privileged EXEC mode:

```
show lldp med-network-policies [port <portlist>] {voice|voice-signaling}
```

### Variable definitions

The following table outlines the parameters of the `show lldp med-network-policies` command.

**Table 94: show lldp med-network-policies parameters**

| 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.           |
| voice-signaling | Specifies the voice signalling network policy to disable.                     |

---

## Configuring LLDP

Use this procedure to configure the LLDP as shown in [LLDP configuration example](#) on page 184.

### ! 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.

### Procedure steps

1. Modify the default LLDP Tx interval from (the default 30 second value) to 60 seconds.  
  
Notice 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 in order to update the peers neighbor tables.
2. Enable the Port Description TLV for transmission. (contains the description of the LLDP 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 could be handled by the LLDP sending port)
15. Configure the location information for the LLDP-MED Location Identification TLV.  
There are three coordinate sets available for location advertisement.
16. 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)  
MED TLVs are transmitted only if MED-Capabilities TLV is transmitted
17. Enable the Network Policy TLV for transmission. (advertises the available MED applications available on the LLDP sending device and the policies required to use the applications)
18. 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)
19. Enable the Extended Power-via-MDI TLV for transmission. (provides detailed informations regarding the PoE parameters of the LLDP sending device)
20. Enable the Inventory – Hardware Revision TLV for transmission. (indicates the hardware revision of the LLDP sending device)
21. Enable the Inventory – Firmware Revision TLV for transmission. (indicates the firmware revision of the LLDP sending device)
22. Enable the Inventory – Software Revision TLV for transmission. (indicates the software revision of the LLDP sending device)
23. Enable the Inventory – Serial Number TLV for transmission. (indicates the serial number of the LLDP sending device)
24. Enable the Inventory – Manufacturer Name TLV for transmission. (indicates the manufacturer name of the LLDP sending device)
25. Enable the Inventory – Model Name TLV for transmission. (indicates the model name of the LLDP sending device)

**\* Note:**

The switch only transmits LLDP MED information if the neighbor is a MED-capable unit.

## 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 or MED TLV from its peers.

shows an example of LLDP configuration. For this example, the router is connected to the ERS 5000 Series port 1 and the IP Phone uses port 13.



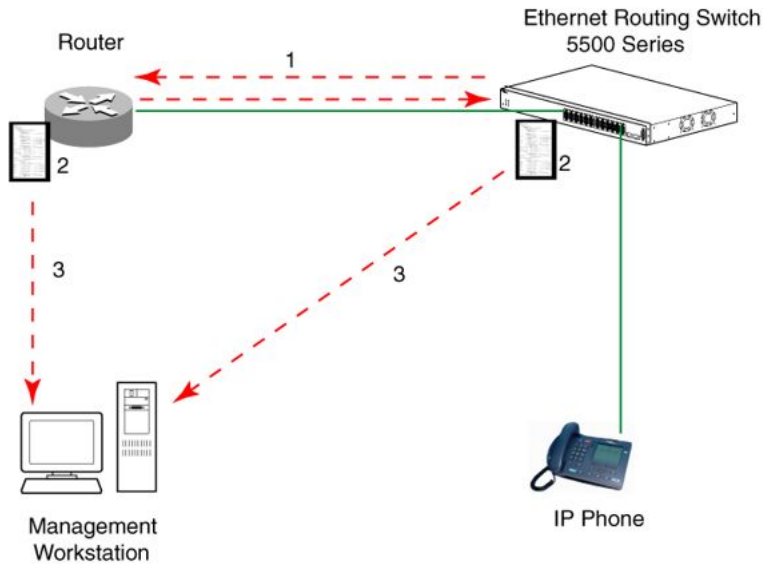


Figure 25: LLDP configuration example

## Detailed configuration commands

The following section describes the detailed ACLI commands required to carry out the configuration depicted in [Figure 25: LLDP configuration example](#) on page 185.

### Navigation:

- [Modifying the default LLDP Tx interval](#) on page 186
- [Checking the new LLDP global settings](#) on page 186
- [Enabling all LLDP Core TLVs for transmission on the router and IP Phone ports](#) on page 186
- [Checking the LLDP settings of the router and IP Phone ports](#) on page 187
- [Enabling all LLDP DOT1 TLVs for transmission on the router and IP Phone ports](#) on page 187
- [Checking the LLDP settings of the router and IP Phone ports](#) on page 187
- [Enabling all LLDP DOT3 TLVs for transmission on the router and IP Phone ports](#) on page 188
- [Checking the LLDP settings of the router and IP Phone ports](#) on page 188
- [Enabling all LLDP MED TLVs for transmission on the router and IP Phone ports](#) on page 189
- [Checking the new LLDP settings of the router and IP Phone ports](#) on page 189

## Modifying the default LLDP Tx interval

Use this procedure to modify the default LLDP Tx interval.

### Procedure steps

Use the following command from Global Configuration mode:

```
lldp tx-interval 60
```

## Checking the new LLDP global settings

Use this procedure to show LLDP global settings.

### Procedure steps

Use the following command from Global Configuration mode:

```
show lldp
```

### Job aid

The following job aid shows the output for the `show lldp` command.

```
5520-24T-PWR(config)#show lldp
```

```
-----  
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

Use this procedure to enable all LLDP Core TLVs for transmission on the route and IP Phone ports.

### Procedure steps

Use the following command from Global Configuration mode:

```
interface fastEthernet 1,13  
lldp tx-tlv port 1,13 port-desc  
lldp tx-tlv port 1,13 sys-name  
lldp tx-tlv port 1,13 sys-desc
```

```
lldp tx-tlv port 1,13 sys-cap
lldp tx-tlv port 1,13 local-mgmt-addr
```

## Checking the LLDP settings of the router and IP Phone ports

Use this procedure to check the LLDP settings of the router and IP Phone ports.

### Procedure steps

Use the following command from Interface Configuration mode:

```
show lldp port 1,13 tx-tlv
```

### Job aid

The following job aid shows the output for the `show lldp port 1,13 tx-tlv` command.

```
5520-24T-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

Use this procedure to enable all LLDP DOT1 TLVs for transmission on the router and IP Phone ports.

### Procedure steps

Use the following command from Interface Configuration mode:

```
lldp tx-tlv port 1,13 dot1 port-vlan-id
lldp tx-tlv port 1,13 dot1 port-protocol-vlan-id
lldp tx-tlv port 1,13 dot1 vlan-name
lldp tx-tlv port 1,13 dot1 protocol-identity EAP
LLDP STP
```

## Checking the LLDP settings of the router and IP Phone ports

Use this procedure to check the LLDP setting of the router and IP Phone ports.

**Procedure steps**

Use the following command from Interface Configuration mode:

```
show lldp port 1,13 tx-tlv dot1
```

**Job aid**

The following job aid shows the output for the `show lldp port 1,13 tx-tlv dot1` command.

```
5520-24T-PWR(config-if)#show lldp port 1,13 tx-tlv dot1
```

```
-----
lldp port dot1 tlvs
-----
Dot1 protocols: STP,EAP,LLDP
-----
Port PortVlanId VlanNameList PortProtocolVlanId ProtocolIdentity
-----
1      true  1                1                ALL
13     true  1                1                ALL
```

**Enabling all LLDP DOT3 TLVs for transmission on the router and IP Phone ports**

Use this procedure to enable all LLDP DOT3 TLVs for transmission on the router and IP Phone ports.

**Procedure steps**

Use the following command from Interface Configuration mode:

```
lldp tx-tlv port 1,13 dot3 mac-phy-config-status
lldp tx-tlv port 1,13 dot3 mdi-power-support
lldp tx-tlv port 1,13 dot3 link-aggregation
lldp tx-tlv port 1,13 dot3 maximum-frame-size
```

**Checking the LLDP settings of the router and IP Phone ports**

Use this procedure to check the LLDP settings of the router and IP Phone ports.

**Procedure steps**

Use the following command from Interface Configuration mode:

```
show lldp port 1,13 tx-tlv dot3
```

### Job aid

The following job aid shows the output for the `show lldp port 1,13 tx-tlv dot3` command.

```
5520-24T-PWR(config-if)#show lldp port 1,13 tx-tlv dot3
```

```
-----
lldp port dot3 tlvs
-----
-----
Port  MacPhy      MdiPower  Link      MaxFrameSize  ConfigStatus  Support
Aggregation
-----
1      true          true      true      true          true
13     true          true      true      true          true
-----
```

## Enabling all LLDP MED TLVs for transmission on the router and IP Phone ports

Use this procedure to enable all LLDP MED TLVs for transmission on the router and IP Phone ports.

### \* Note:

The first three commands are required to configure the location identification for the LLDP-MED Location Identification TLV.

### Procedure steps

Use the following command from Interface Configuration mode:

```
lldp location-identification civic-address country-code US city
Boston

lldp location-identification coordinate-base altitude 3 floors

lldp location-identification ecs-elin 1234567890

lldp tx-tlv med port 1,13 med-capabilities

lldp tx-tlv med port 1,13 network-policy

lldp tx-tlv med port 1,13 location

lldp tx-tlv med port 1,13 extendedPSE

lldp tx-tlv med port 1,13 inventory
```

## Checking the new LLDP settings of the router and IP Phone ports

Use this procedure to check the new LLDP settings of the router and IP Phone ports.

## Procedure steps

Use the following command from Interface Configuration mode:

```
show lldp tx-tlv med
```

## Job aid

The following job aid shows the output of the `show lldp tx-tlv med` command.

```
5530-24TFD(config-if)#show lldp tx-tlv med
```

```

-----
lldp port med tlvs
-----
-----
Port Med      Network Location Extended Inventory Capabilities
Policy                PSE
-----
1      true     true   true   true   true
13     true     true   true   true   true
-----

```

---

# Configuring PoE detection method with ACLI

---

## Configuring PoE with ACLI

The following section details the commands necessary to configure PoE with ACLI:

- [Set port power enable or disable](#) on page 190
- [Set port power priority](#) on page 191
- [Set power limit for channels](#) on page 191
- [Set traps control](#) on page 192
- [Show main power status](#) on page 192
- [Set power usage threshold](#) on page 192
- [Setting PoE detection method](#) on page 193
- [Show port power status](#) on page 193
- [Show port power measurement](#) on page 194

---

## Set port power enable or disable

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

**Procedure steps**

Use the following command from Interface Configuration mode:

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

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

**Procedure steps**

Use the following command from Interface Configuration mode:

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

**\* Note:**

In either command, substitute **<portlist>** with the ports on which PoE is enabled or disabled.

**Set port power priority**

Use this procedure to set the port power priority.

**Procedure steps**

Use the following command from Interface Configuration mode:

```
poe poe-priority [port <portlist>] {critical | high | low}
```

**Variable definitions**

The following table outlines the parameters of the **poe-priority** command.

**Table 95: poe-priority command parameters**

| Variable                | Value                          |
|-------------------------|--------------------------------|
| port <portlist>         | The ports to set priority for. |
| {low   high   critical} | The PoE priority for the port. |

**Set power limit for channels**

Use this procedure to set the power limit for channels.

**Procedure steps**

Use the following command from Interface Configuration mode:

```
poe poe-limit [port <portlist>] <3-16>
```

## Variable definitions

The following table outlines the parameters of the `poe-limit` command.

**Table 96: poe-limit command parameters**

| Variable        | Value                                           |
|-----------------|-------------------------------------------------|
| port <portlist> | The ports to set the limit on.                  |
| <3 - 16>        | The power range to limit at from 3 to 16 Watts. |

---

## Set traps control

Use this procedure to enable PoE-related traps for PoE-enabled ports.

### Procedure steps

Use the following command from Interface Configuration mode:

```
poe poe-trap [unit <1-8>]
```

**\* Note:**

Substitute <1-8> with the number of the unit on which to enable traps.

---

## Show main power status

Use this procedure to display the power configuration.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
show poe-main-status [unit <1-8>]
```

**\* Note:**

Substitute <1-8> with the number of the unit for which to display the configuration.

---

## Set power usage threshold

Use this procedure to set the power usage threshold in percentage on individual units.



## Procedure steps

Use the following command from Global Configuration mode:

```
poe poe-power-usage-threshold [unit <1-8>] <1-99>
```

## Variable definitions

The following table outlines the parameters of the `poe-power-usage-threshold` command.

**Table 97: poe-power-usage-threshold command parameters**

| Variable     | Value                                          |
|--------------|------------------------------------------------|
| unit <1 - 8> | The unit for which to set the power threshold. |
| <1 - 99>     | 1--99 percent                                  |

---

## Setting PoE detection method

Use this procedure to enable either 802.3af or Legacy compliant PD detection methods.

### Procedure steps

Use the following command from Global Configuration mode:

```
poe poe-pd-detect-type [unit <1-8>] {802dot3af | 802dot3af_and_legacy}
```

---

## Show port power status

Use this procedure to display the power configuration.

### Procedure steps

Use the following command from Global Configuration mode:

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

**\* Note:**

Substitute `<portlist>` with the ports for which to display configuration.

---

## Show port power measurement

Use this procedure to display the configuration.

### Procedure steps

Use the following command from Global Configuration mode:

```
show poe-power-measurement [<portlist>]
```

**\* Note:**

Substitute <portlist> with the ports for which to display configuration.

---

## Customizing ACLI banner with ACLI

The following sections show the commands used to customize the ACLI banner.

### Navigation:

- [show banner command](#) on page 194
- [banner command](#) on page 195
- [no banner command](#) on page 195

---

## show banner command

Use this procedure to display the banner.

### Procedure steps

Use the following command from Privileged EXEC mode:

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

## Variable definitions

The following table outlines the parameters of the `show banner` command.

**Table 98: show banner command parameters**

| Variable        | Value                                              |
|-----------------|----------------------------------------------------|
| static   custom | Displays which banner is currently set to display: |

| Variable | Value                                                                        |
|----------|------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• static</li> <li>• custom</li> </ul> |

---

## banner command

Use this procedure to specify the banner displayed at startup.

### Procedure steps

Use the following command from Privileged EXEC mode:

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

## Variable definitions

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

**Table 99: banner command parameters**

| Variable        | Value                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------|
| static   custom | Sets the display banner as: <ul style="list-style-type: none"> <li>• static</li> <li>• custom</li> </ul> |
| line number     | Enter the banner line number you are setting. The range is 1 to 19.                                      |
| LINE            | Specifies the characters in the line number.                                                             |

---

## no banner command

Use this procedure to clear all lines of a previously stored custom banner.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
no banner
```

**\* Note:**

This command sets the banner type to the default setting (STATIC).

---

## Displaying complete GBIC information

Use this procedure to display complete GBIC information.

### Procedure steps

Use the following command in any command mode:

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

**\* Note:**

Substitute <port-list> with the GBIC ports for which to display information. If no GBIC is detected, this command does not show any information.

---

## Displaying hardware information

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

### Procedure steps

Use the following command from any command mode:

```
show system [verbose]
```

**\* Note:**

The inclusion of the [verbose] option displays additional information about fan status, power status, and switch serial number.

---

## Configuring AUR with ACLI

Use the following commands to configure AUR with ACLI:

- [show stack auto-unit-replacement command](#) on page 197
- [stack auto-unit-replacement enable command](#) on page 198
- [no stack auto-unit-replacement enable command](#) on page 198
- [default stack auto-unit-replacement enable command](#) on page 198
- [stack auto-unit-replacement config save enable](#) on page 198

- [stack auto-unit-replacement config save disable](#) on page 198
- [stack auto-unit-replacement config restore unit](#) on page 199
- [stack auto-unit-replacement config save unit](#) on page 199

---

## show stack auto-unit-replacement command

Use this procedure to display the current AUR settings.

### Procedure steps

Use the following command from any command mode:

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

### Variable definitions

**Table 100: show stack auto-unit-replacement command parameters**

| Variable                           | Value                                                                                                                                                                                                |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 non base unit will be automatically saved to the base unit.                                                                                                   |
|                                    | Disable: The current configuration of a non base unit 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 has been 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 with ACLI](#) on page 196.

For information about configuring AUR with Enterprise Device Manager, see [Configuring AUR](#) on page 225.

---

## stack auto-unit-replacement enable command

Use this procedure to enable AUR on the switch.

### Procedure steps

Use the following command from Global Configuration mode:

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

---

## no stack auto-unit-replacement enable command

Use this procedure to disable AUR on the switch.

### Procedure steps

Use the following command from Global Configuration mode:

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

---

## default stack auto-unit-replacement enable command

Use this procedure to restore the default AUR settings.

### Procedure steps

Use the following command from Global Configuration mode:

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

---

## stack auto-unit-replacement config save enable

Use this procedure to enable automatic configuration saves for non-base units.

### Procedure steps

Use the following command from Global Configuration mode:

```
stack auto-unit-replacement config save enable
```

---

## stack auto-unit-replacement config save disable

Use this procedure to disable automatic configuration saves for non-base units.

### Procedure steps

Use the following command from Global Configuration mode:

```
stack auto-unit-replacement config save disable
```

---

## stack auto-unit-replacement config restore unit

Use this procedure to restore the saved configuration to a non-base unit. Use the base unit console in Privileged Mode to enter this command.

### Procedure steps

Use the following command from Privileged EXEC mode:

```
stack auto-unit-replacement config restore unit <1-8>
```

---

## stack auto-unit-replacement config save unit

Use this procedure to save the configuration of the selected non-base unit to the base unit, regardless of the state of the AUR feature.

Use the following command from Privileged EXEC mode:

```
stack auto-unit-replacement config save unit <1-8>
```

---

## Agent Auto Unit Replacement (AAUR)

Use the following commands to configure and use AAUR.

### Navigation:

- [stack auto-unit-replacement-image enable command](#) on page 199
- [no stack auto-unit-replacement-image-enable command](#) on page 200
- [default stack auto-unit-replacement-image enable command](#) on page 200
- [show stack auto-unit-replacement-image command](#) on page 200

---

## stack auto-unit-replacement-image enable command

Use this procedure to enable AAUR.

### Procedure steps

Use the following command from Global Configuration mode:

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

**\* Note:**

AAUR is enabled by default; this command is only used if this functionality was previously disabled.

---

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

Use this procedure to disable AAUR.

### Procedure steps

Use the following command from Global Configuration mode:

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

**\* Note:**

AAUR is enabled by default; this command must be executed if the AAUR functionality is not desired on a switch.

---

## default stack auto-unit-replacement-image enable command

Use this procedure to set the AAUR functionality to the factory default of enabled.

### Procedure steps

Use the following command from Global Configuration mode:

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

---

## show stack auto-unit-replacement-image command

Use this procedure to view the current status of the AAUR functionality.

### Procedure steps

Use the following command from User EXEC mode:



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

---

## Enabling Autosave

With autosave enabled the system checks every minute to see if there is any new configuration data. If there is, it will automatically be saved to NVRAM. While autosave is enabled, the AUR feature should perform normally.

Use the following command to enable the autosave feature.

---

### autosave enable command

Use this procedure to enable the autosave feature.

#### Procedure steps

Use the following command from Global Configuration mode:

```
autosave enable
```

---

## Disabling Autosave

With autosave disabled, the unit will not save the new configuration data to NVRAM. The user can restore via AUR all the configuration data that is configured before the feature is disabled. The user can also restore via AUR all the configuration data that is configured before ACLI command `copy config nvram` is executed.

When resetting a stack with autosave disabled the stack will form with the configuration from NVRAM of each unit in the stack. The original configuration of a unit should be restored if the user replaces that unit in the stack without having to use the `copy config nvram` command.

---

### no autosave enable command

Use this procedure to disable the autosave feature.

#### Procedure steps

Use the following command from Global Configuration mode:

```
no autosave enable
```

---

## 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 this procedure to configure stack forced-mode.:

### Procedure steps

Use the following command from Global Configuration mode:

```
<no | default | show>
```

---

## Variable definitions

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

**Table 101: stack forced-mode command parameters**

| Variable | Value                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <>       | 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: <ul style="list-style-type: none"> <li>• Forced-Stack Mode: Enabled Device is not currently running in forced Stack Mode.</li> <li>• Forced-Stack Mode: Enabled Device is currently running in forced Stack Mode.</li> <li>• Forced-Stack Mode: Disabled Device is not currently running in forced Stack Mode.</li> </ul> |

---

## Enabling feature license files

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

- [copy tftp license command](#) on page 203
- [show license command](#) on page 204
- [clear license command](#) on page 204

---

### copy tftp license command

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

#### Procedure steps

Use the following command from Privileged EXEC mode:

```
copy tftp license <A.B.C.D> <WORD>
```

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

With the `copy tftp license <A.B.C.D.> <WORD>` command, you can copy the features software license file from a TFTP server to your switch.

#### \* Note:

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

### Variable definitions

The following table outlines the parameters of the `copy tftp license` command.

**Table 102: copy tftp license command parameters**

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

---

## show license command

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

### Procedure steps

Use the following command from Privileged EXEC mode:

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

---

## clear license command

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

### Procedure steps

Use the following command from Privileged EXEC mode:

```
clear license { <1-10> / all }
```

---

## Setting user access limitations

The following sections show the commands for setting user access limitations.

### Navigation:

- [Setting the read-only and read-write passwords](#) on page 204
- [Enabling and disabling passwords](#) on page 205
- [Configuring RADIUS authentication](#) on page 206
- [Related RADIUS Commands](#) on page 207

---

## Setting the read-only and read-write passwords

The first step to requiring password authentication when the user logs in to the switch is to edit the password settings..

Use this procedure to se the read-only and read-write passwords.

### Procedure steps

Use the following command from Privileged EXEC mode:

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

## Variable definitions

The following table outlines the parameters of the `cli password` command.

**Table 103: cli password command parameters**

| Variable                 | Value                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| {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. |

## Enabling and disabling passwords

After the read-only and read-write passwords are set, they can be individually enabled or disabled for the various switch access methods. When enabled, password security prompts you for a password and the value is hidden.

Use this procedure to enable or disable passwords.

### Procedure steps

Use the following command from Privileged EXEC mode:

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

## Variable definitions

The following table outlines the parameters of the `cli password` command.

**Table 104: cli password command parameters**

| Variable                         | Value                                                                                                                                                                                                                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {telnet   serial}                | This parameter specifies if the password is enabled or disabled for telnet or the console.                                                                                                                                                                                          |
| {none   local   radius   tacacs} | This parameter specifies if the password is to be disabled (none), or if the password to be used is the locally stored password created in <a href="#">Setting the read-only and read-write passwords</a> on page 204, or if RADIUS authentication or TACACS +AAA services is used. |

## Configuring RADIUS authentication

The Remote Authentication Dial-In User Service (RADIUS) protocol is a means to authenticate users through the use of a dedicated network resource. This network resource contains a listing 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, when prompted, a password. The password value is hidden when entered. This information is checked against the preexisting list. If the user credentials are valid they can access the switch.

If RADIUS Authentication was selected when enabling passwords through ACLI, the RADIUS server settings must be specified to complete the process.

Use this procedure to enable RADIUS authentication.

### Procedure steps

Use the following command from Global Configuration mode:

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

## Variable definitions

The following table outlines the parameters of the `radius-server` command.

**Table 105: radius-server command parameters**

| Variable                   | Value                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <address>             | This parameter is the IPv6 or IPv4 address of the RADIUS server that is used for authentication.                                                                                                                                              |
| [secondary-host <address>] | The secondary-host <address> parameter is optional. If a backup RADIUS server is to be specified, include this parameter with the IPv6 or IPv4 address of the backup server.                                                                  |
| port <num>                 | This parameter is the UDP port number the RADIUS server uses to listen for requests.                                                                                                                                                          |
| key                        | This parameter prompts you to supply a secret text string or password that is shared between the switch and the RADIUS server. Enter the secret string, which is a string up to 16 characters in length. The password is hidden when entered. |
| [password fallback]        | This parameter is optional and enables the password fallback feature on the RADIUS server. This option is disabled by default.                                                                                                                |

---

## Related RADIUS Commands

During the process of configuring RADIUS authentication, there are three other CLI commands that can be useful to the process. These commands are:

- **show radius-server** —The command takes no parameters and displays the current RADIUS server configuration.
- **no radius-server**—This command takes no parameters and clears any previously configured RADIUS server settings.
- **radius-server password fallback**—This command takes no parameters and enables the password fallback RADIUS option if it was not done when the RADIUS server was configured initially.

---

## Configuring serial console port and USB host port

You can enable or disable the serial console and USB host ports to control access to an operational switch. Disabling the USB or serial console ports can prevent unauthorized access and configuration. Both the serial console and USB host ports are enabled by default. CLI and ACG are used to enable and disable the serial console and USB host ports. ACG support allows users to save the current settings as text files using CLI commands.

While disabled, the USB host port does not provide power to attached USB devices. No operation which uses the USB host port will be able to complete.

While disabling a console port, the current session ends. While it is disabled and the device is rebooted, the banner is no longer displayed. After enabling the port the user will see the login banner.

If the **show running config** command is running while disabling the serial console port, the execution is aborted.

The following CLI commands are used to enable and disable the serial console port and the USB host port:

### Navigation:

- [serial-console command](#) on page 208
- [no serial-console command](#) on page 208
- [default serial-console command](#) on page 209
- [show serial-console command](#) on page 209
- [usb-host-port command](#) on page 209
- [no usb-host-port command](#) on page 210

- [default usb-host-port command](#) on page 210
- [show usb-host-port](#) on page 211

---

## serial-console command

Use this procedure to enable serial console ports to grant users console access.

### Procedure steps

Use the following command from Global Configuration mode:

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

### Variable definitions

The following table outlines the parameters of the `serial-console` command.

**Table 106: serial-console command parameters**

| Variable     | Value                                                            |
|--------------|------------------------------------------------------------------|
| [unit <1-8>] | Identifies the unit number in a stack. Values range from 1 to 8. |

---

## no serial-console command

Use this procedure to disable the serial console port to deny users console access.

### Procedure steps

Use the following command from Global Configuration mode:

```
no serial-console [unit <1-8>] [enable]
```

### Variable definitions

The following table outlines the parameters of the `no serial-console` command.

**Table 107: no serial-console command parameters**

| Variable     | Value                                                            |
|--------------|------------------------------------------------------------------|
| [unit <1-8>] | Identifies the unit number in a stack. Values range from 1 to 8. |



---

## default serial-console command

Use this procedure to reset the serial console port to its default setting of enabled.

### Procedure steps

Use the following command from Global Configuration mode:

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

## Variable definitions

The following table outlines the parameters of the **default serial-console** command.

**Table 108: default serial-console command parameters**

| Variable     | Value                                                            |
|--------------|------------------------------------------------------------------|
| [unit <1-8>] | Identifies the unit number in a stack. Values range from 1 to 8. |

---

## show serial-console command

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

### Procedure steps

Use the following command from Privileged EXEC mode:

```
show serial-console command [unit <1-8>]
```

## Variable definitions

The following table outlines the parameters of the **show serial-console** command.

**Table 109: show serial-console command parameters**

| Variable     | Value                                                            |
|--------------|------------------------------------------------------------------|
| [unit <1-8>] | Identifies the unit number in a stack. Values range from 1 to 8. |

---

## usb-host-port command

Use this procedure to enable USB ports to grant users console access.

## Procedure steps

Use the following command from Global Configuration mode:

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

## Variable definitions

The following table outlines the parameters of the `usb-host-port` command.

**Table 110: usb-host-port command parameters**

| Variable     | Value                                                            |
|--------------|------------------------------------------------------------------|
| [unit <1-8>] | Identifies the unit number in a stack. Values range from 1 to 8. |

---

## no usb-host-port command

Use this procedure to disable the USB host port to deny users console access.

### Procedure steps

Use the following command from Global Configuration mode:

```
no usb-host-port [unit <1-8>] [enable]
```

## Variable definitions

The following table outlines the parameters of the `no usb-host-port` command.

**Table 111: no usb-host-port command parameters**

| Variable     | Value                                                            |
|--------------|------------------------------------------------------------------|
| [unit <1-8>] | Identifies the unit number in a stack. Values range from 1 to 8. |

---

## default usb-host-port command

Use this procedure to reset the USB host port to its default setting of enabled.

### Procedure steps

Use the following command from Global Configuration mode:

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

## Variable definitions

The following table outlines the parameters of the `default usb-host-port` command.

**Table 112: default usb-host-port command parameters**

| Variable     | Value                                                            |
|--------------|------------------------------------------------------------------|
| [unit <1-8>] | Identifies the unit number in a stack. Values range from 1 to 8. |

---

## show usb-host-port

Use this procedure to display the operational status of the USB ports on all switches.

### Procedure steps

Use the following command from Global Configuration mode:

```
show usb-host-port
```

---

## Restoring factory default

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

### Procedure steps

Use the following command from Global Configuration mode:

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

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



# Chapter 7: System configuration with Enterprise Device Manager

This section contains information about the following topics:

- [Configuring Quick Start using EDM](#) on page 214
- [Configuring remote access using EDM](#) on page 214
- [Configuring the IPv4 remote access list using EDM](#) on page 215
- [Configuring the IPv6 remote access list using EDM](#) on page 216
- [Viewing PoE ports with Enterprise Device Manager](#) on page 217
- [General Switch Administration with Enterprise Device Manager](#) on page 218
- [Avaya Energy Saver configuration using Enterprise Device Manager](#) on page 244
- [Bridge configuration using Enterprise Device Manager](#) on page 253
- [File System configuration using Enterprise Device Manager](#) on page 256
- [ADAC Configuration using Enterprise Device Manager](#) on page 267
- [Topology configuration using Enterprise Device Manager](#) on page 270
- [System Log configuration using Enterprise Device Manager](#) on page 272
- [LLDP configuration using Enterprise Device Manager](#) on page 275
- [LLDP Port dot1 configuration using Enterprise Device Manager](#) on page 291
- [LLDP Port dot3 configuration using Enterprise Device Manager](#) on page 297
- [LLDP Port MED configuration using Enterprise Device Manager](#) on page 304
- [SNTP configuration using Enterprise Device Manager](#) on page 323
- [Power over Ethernet configuration with Enterprise Device Manager](#) on page 327
- [IPv6 configuration using Enterprise Device Manager](#) on page 330
- [Viewing SFP GBIC ports](#) on page 332

---

## Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

---

## 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** .

Use the data in this table to configure remote access for a switch.

**Table 113: Variable definitions**

| Variable                       | Value                                                                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet Remote Access Setting   | Specifies the remote access settings for telnet sessions. <ul style="list-style-type: none"> <li>• Access—allows or disallows telnet access to the switch</li> <li>• Use List—enables (Yes) or disables (No) the use of listed remote Telnet information.</li> </ul> |
| SNMP Remote Access Setting     | Specifies SNMP remote access settings. <ul style="list-style-type: none"> <li>• Access—allows or disallows SNMP access to the switch</li> <li>• Use List—enables (Yes) or disables (No) the use of listed remote SNMP information.</li> </ul>                        |
| Web Page Remote Access Setting | Specifies web page remote access settings. <ul style="list-style-type: none"> <li>• Use List—enables (Yes) or disables (No) the use of listed remote web page information.</li> </ul>                                                                                |
| SSH Remote Access Setting      | Specifies SSH remote access settings. <ul style="list-style-type: none"> <li>• Access—allows or disallows SSH access to the switch</li> <li>• Use List—enables (Yes) or disables (No) the use of listed remote SSH information.</li> </ul>                           |

---

## 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**.

Use the data in this table to configure to configure a list of IPv4 source addresses for which to permit access to the switch.

**Table 114: Variable definitions**

| 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** .

Use the data in this table to configure to configure a list of IPv6 source addresses for which to permit access to the switch .

**Table 115: Variable definitions**

| 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 PoE ports with Enterprise Device Manager

The Front Panel view of Enterprise Device Manager provides additional information for PoE ports on the Avaya Ethernet Routing Switch 5520. This additional information is provided 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.

[Figure 26: Avaya Ethernet Routing Switch 5520-48T-PWR](#) on page 217 displays an example of the Front Panel view of an Avaya Ethernet Routing Switch 5520-48T-PWR.



**Figure 26: Avaya Ethernet Routing Switch 5520-48T-PWR**

[Table 116: Power Aspect color codes](#) on page 217 explains what the different colors displayed by the power aspect represent.

**Table 116: Power Aspect color codes**

| Color | Description                                                                |
|-------|----------------------------------------------------------------------------|
| Green | Indicates that the port is currently delivering power.                     |
| Red   | Indicates that the power and detection mechanism for the port is disabled. |

| Color      | Description                                                                                                           |
|------------|-----------------------------------------------------------------------------------------------------------------------|
| Orange     | Indicates that the power and detection mechanism for the port is enabled. The port is not currently delivering power. |
| White/Gray | Indicates that the power and detection mechanism for the port is unknown.                                             |

**\* Note:**

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

For more information about PoE, see the following sections:

- [Displaying the PoE tab for a single unit](#) on page 219
- [Viewing the PoE power settings](#) on page 234

---

## General Switch Administration with Enterprise Device Manager

This section contains information about the following topics:

- [Displaying the Unit dialog box](#) on page 218
- [Displaying the Chassis dialog box](#) on page 221
- [Displaying the Switch/Stack dialog box](#) on page 226
- [Displaying the Ports dialog box](#) on page 230
- [Displaying the Environment dialog box](#) on page 242

---

### Displaying the Unit dialog box

The Power over Ethernet (PoE) parameters that apply to the whole switch can be configured and viewed using the Unit screen.

**\* Note:**

View and edit the PoE parameters for each Avaya Ethernet Routing Switch 5520 one by one. If more than one unit is selected, the PoE power parameters, such as the PoE tab, are not displayed.

To open the Unit dialog box:

## Procedure steps

1. In the **Device Physical View**, select the unit.
2. From the navigation tree, double-click **Edit**.
3. From the Edit tree, double-click **Unit**.

This sections contains information about the following topics:

- [Displaying the Unit tab for a single unit](#) on page 219
- [Displaying the PoE tab for a single unit](#) on page 219

## Displaying the Unit tab for a single unit

To display the Unit tab for a single unit:

### Procedure steps

1. In the **Device Physical View**, select the unit.
2. From the navigation tree, double-click **Edit**.
3. From the Edit tree, double-click **Unit**.
4. Select the **Unit** tab.

The following table outlines the parameters for the **Unit** tab.

**Table 117: Variable definitions**

| Variable      | Value                                      |
|---------------|--------------------------------------------|
| Type          | Specifies the type number.                 |
| Descr         | Specifies the type of switch.              |
| Ver           | Specifies the version number of the switch |
| SerNum        | Specifies the serial number of the switch. |
| BaseNumPorts  | Specifies the base number of ports.        |
| TotalNumPorts | Specifies the total number of ports.       |

## Displaying the PoE tab for a single unit

To set the power usage threshold, the power pairs to use, and the power detection method to use, select a single Avaya Ethernet Routing Switch 5520 unit.

### \* Note:

These parameters only can be viewed and set by selecting a single unit. If more than one unit is selected, the **PoE** tab is not displayed.

To open the PoE tab for a single unit:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Unit**.
3. Select the **PoE** tab.

The following table outlines the parameters of the **PoE** tab.

**Table 118: Variable definitions**

| Variable                    | Value                                                                                                                                                                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power                       | Displays the total power available to the Avaya Ethernet Routing Switch 5520.                                                                                                                                                                                            |
| OperStatus                  | Displays the power state of the Avaya Ethernet Routing Switch 5520.: <ul style="list-style-type: none"> <li>• on</li> <li>• off</li> <li>• faulty</li> </ul>                                                                                                             |
| Consumption Power           | Displays the power being used by the Avaya Ethernet Routing Switch 5520.                                                                                                                                                                                                 |
| Usage Threshold             | Enables you to set a percentage of the total power usage of the Avaya Ethernet Routing Switch 5520 switch based on which the system sends a trap. <p><b>Note:</b><br/>You must have the traps enabled (see NotificationControlEnable) to receive a power usage trap.</p> |
| Notification Control Enable | Enables you to enable or disable sending traps if the switch's power usage exceed the percentage set in the UsageThreshold field.                                                                                                                                        |
| PowerDevice DetectType      | Enables you to set the power detection method that the switch uses to detect a request for power from a device connected to all ports on the switch: <ul style="list-style-type: none"> <li>• 802.3af</li> <li>• 802.3af and legacy</li> </ul>                           |
| PowerPairs                  | Displays the RJ-45 pin pairs that the switch uses to send power to the ports on the switch.                                                                                                                                                                              |

## Displaying the Chassis dialog box

To open the Chassis dialog box:

### Procedure steps

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

The following sections provide a description of the tabs in the Edit Chassis screen:

- [Viewing system properties](#) on page 221
- [Displaying the Asset ID tab](#) on page 223
- [Displaying the Banner tab](#) on page 223
- [Displaying the Custom Banner tab](#) on page 224
- [Viewing stack mode properties](#) on page 225
- [Configuring AUR](#) on page 225

## Viewing system properties

Use the System tab to specify, among other things, tracking information for a device and device descriptions.

To view the System tab:


### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Chassis**.
4. Select the **System** tab.

The following table outlines the parameters for the **System** tab.

**Table 119: Variable definitions**

| Variable    | Value                                      |
|-------------|--------------------------------------------|
| sysDescr    | A description of the device.               |
| sysUpTime   | The time since the system was last booted. |
| sysObjectID | The system object identification number.   |

| Variable                 | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sysContact               | Type the contact information (in this case, an e-mail address) for the system administrator.                                                                                                                                                                                                                                                                                                                                                               |
| sysName                  | Type the name of this device.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| sysLocation              | Type the physical location of this device.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| AuthenticationTraps      | <p>Click to enable or disable. When you select enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When you select disabled, no traps are received.</p> <p>To view traps, click the Trap toolbar button.</p>                                                                                                                               |
| Reboot                   | <p>Action object to reboot the agent.</p> <p>Reset -- initiates a hardware reset.</p> <p>The agent attempts to return a response before the action occurs. If any of the combined download actions are requested, neither action occurs until the expiration of s5AgInfoScheduleBootTime, if set.</p> <ul style="list-style-type: none"> <li>• bootPrimary: Use the primary boot image.</li> <li>• bootSecondary: Use the secondary boot image.</li> </ul> |
| AutoPvid                 | Click enabled or disabled. When you select enabled, Port VLAN ID (PVID) is automatically assigned.                                                                                                                                                                                                                                                                                                                                                         |
| StackInsertionUnitNumber | The unit number to be assigned to the next unit that joins the stack. The value cannot be set 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 when determining the unit number of new units.                                                                                            |
| JumboFramesEnabled       | Click to enable or disable jumbo frames.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| NextBootMgmtProtocol     | The transport protocols to use after the next boot of the agent.                                                                                                                                                                                                                                                                                                                                                                                           |
| CurrentMgmtProtocol      | Read only: The current transport protocols that the agent supports.                                                                                                                                                                                                                                                                                                                                                                                        |
| BootMode                 | <p>The source from which to load the initial protocol configuration information to boot the switch the next time. The options available are</p> <ul style="list-style-type: none"> <li>• bootpDisabled</li> <li>• bootpAlways</li> <li>• bootpWhenNeeded</li> <li>• bootpOrLastAddress</li> <li>• dhcp</li> </ul>                                                                                                                                          |

| Variable               | Value                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                        | <ul style="list-style-type: none"> <li>• dhcpWhenNeeded</li> <li>• dhcpOrLastAddress</li> </ul>                                 |
| CurrentImageVersion    | Read only: The version number of the agent image that is currently used on the switch.                                          |
| NextBootDefaultGateway | Read only: The IP address of the default gateway for the agent to use after the next time the switch is booted.                 |
| CurrentDefaultGateway  | Read only: The IP address of the default gateway that is currently in use.                                                      |
| NextBootLoadProtocol   | Read only: The transport protocol to be used by the agent to load the configuration information and the image at the next boot. |
| LastLoadProtocol       | Read only: The transport protocol last used to load the image and configuration information about the switch.                   |

## Displaying the Asset ID tab

To open the Asset ID tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Chassis**.
4. Select the **Asset ID** tab.

The following table outlines the parameters for the **Asset ID** tab.

**Table 120: Variable definitions**

| Variable | Value                                                                                      |
|----------|--------------------------------------------------------------------------------------------|
| Class    | Specifies the local MED device class.                                                      |
| AssetID  | Specifies the vendor-specific asset tracking identifier as advertised by the local device. |

## Displaying the Banner tab

To display the Banner tab:

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Chassis**.
4. Select the **Banner** tab.

The following table outlines the parameters for the **Banner** tab.

**Table 121: Variable definitions**

| Variable      | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BannerControl | <p>BannerControl specifies the banner to be displayed as soon as you connect to an Avaya Ethernet Routing Switch 5000 Series device. BannerControl has the following three options:</p> <ul style="list-style-type: none"> <li>• The static option causes the predefined static banner to be used.</li> <li>• The custom option causes the previously set custom banner to be used when displaying a banner.</li> <li>• The disabled option prevents the display of any banners.</li> </ul> |

## Displaying the Custom Banner tab

To display the Custom Banner tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Chassis**.
4. Select the **Custom Banner** tab.

The following table outlines the parameters for the **Custom Banner** tab.

**Table 122: Variable definitions**

| Variable | Value                                                                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type     | Identifies the banner type. There are two types of banner - one type is used in switch or stand-alone mode while the other is used in the stack mode.       |
| Id       | Identifies the line of text within a custom banner                                                                                                          |
| Line     | Displays a one line of a fifteen line banner. If the line contains non-printable ASCII characters, then the line is rejected and an error message returned. |



## Viewing stack mode properties

To view the Stack Mode tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Chassis**.
4. Select the **Stack Mode** tab.

The following table outlines the parameters for the **Stack Mode** tab.

**Table 123: Variable definitions**

| Variable               | Value                     |
|------------------------|---------------------------|
| CurrentOperationalMode | View operational mode.    |
| NextBootOperationMode  | View boot operation mode. |

## Configuring AUR

To configure AUR:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Chassis**.
4. Select the **AUR** tab.
5. Enable Auto Unit Replacement by selecting the **AutoUnitReplacementEnabled** check box.
6. Enable Auto Unit Replacement saving by selecting the **AutoUnitReplacementSaveEnabled** check box.
7. Enter a value for forced saves in the **AutoUnitReplacementForceSaves** field.
8. Enter a value for AUR restore in the **AutoUnitReplacementRestore** field.
9. Click **Apply**.

The following table outlines the parameters for the **AUR** tab.

**Table 124: Variable definitions**

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

---

## Displaying the Switch/Stack dialog box

The following section provides information about how to display switch/stack details.

- [Displaying the Base Unit Info tab](#) on page 226
- [Viewing stack operating status](#) on page 227
- [Renumbering stack switch units using EDM](#) on page 229

## Displaying the Base Unit Info tab

The Base Unit Info tab provides read-only information about the operating status of the hardware and whether or not the default factory settings are being used.

To display the Base Unit Info tab:


### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Switch/Stack**.
4. Select the **Base Unit Info** tab.

The following table outlines the parameters for the **Base Unit Info** tab.

**Table 125: Variable definitions**

| Variable | Value                                                                                   |
|----------|-----------------------------------------------------------------------------------------|
| Type     | The switch type.                                                                        |
| Descr    | A description of the switch hardware, including number of ports and transmission speed. |

| Variable           | Value                                                                                                                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ver                | The switch hardware version number.                                                                                                                                                                                                                   |
| SerNum             | The switch serial number.                                                                                                                                                                                                                             |
| LstChng            | 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.                             |
| AdminState         | Administrative state of the switch. Select either <b>enable</b> or <b>reset</b> .<br><br> <b>Note:</b><br>In a stack configuration, Reset only resets the base unit. |
| OperState          | The operational state of the switch.                                                                                                                                                                                                                  |
| Location           | Type the physical location of the switch.                                                                                                                                                                                                             |
| RelPos             | The relative position of the switch.                                                                                                                                                                                                                  |
| BaseNumPorts       | The number of base ports of the switch.                                                                                                                                                                                                               |
| TotalNumPorts      | The number of ports of the switch.                                                                                                                                                                                                                    |
| IpAddress          | The base unit IP address.                                                                                                                                                                                                                             |
| RunningSoftwareVer | The software version.                                                                                                                                                                                                                                 |

## Viewing stack operating status

The Stack Info tab provides read-only information about the operating status of the stacked switches and whether or not the default factory settings are being used.

To open the Stack Info tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Switch/Stack**.
4. Select the **Stack Info** tab.

The following table outlines the parameters for the **Stack Info** tab.

**Table 126: Variable definitions**

| Variable | Value                                                                                                |
|----------|------------------------------------------------------------------------------------------------------|
| Descr    | A description of the component or subcomponent. If not available, the value is a zero length string. |

| Variable   | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location   | <p>The geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected together to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: 4th flr wiring closet in blg A.</p> <p>Notes: 1. This field is applicable only to components that can be found in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in Board or Unit group, the value is a zero length string.</p> <p>2. If this field is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value defaults to the value of the object s5ChasComSerNum.</p> |
| LstChng    | <p>The value of sysUpTime when it was detected that the component/sub-component was added to the chassis. If this action has not occurred since the cold/warm start of the agent, then the value is zero.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| AdminState | <p>The state of the component or subcomponent.<br/>The values that are read-only are:</p> <ul style="list-style-type: none"> <li>• other -- currently in some other state</li> <li>• notAvail -- actual value is not available</li> </ul> <p>The possible values that can be read and written are:</p> <ul style="list-style-type: none"> <li>• enable--enables operation</li> <li>• reset--resets component</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                            |
| OperState  | <p>The current operational state of the component. The possible values are:</p> <ul style="list-style-type: none"> <li>• other--some other state</li> <li>• notAvail--state not available</li> <li>• removed--component removed</li> <li>• disabled--operation disabled</li> <li>• normal--normal operation</li> <li>• resetInProg--reset in progress</li> <li>• testing--doing a self test</li> <li>• warning--operating at warning level</li> <li>• nonFatalErr--operating at error level</li> <li>• fatalErr--error stopped operation</li> </ul> <p>The allowable (and meaningful) values are determined by the component type.</p>                                                                                                                                                                                             |

| Variable           | Value                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------|
| Ver                | The version number of the component or subcomponent. If not available, the value is a zero length string. |
| SerNum             | The serial number of the component or subcomponent. If not available, the value is a zero length string.  |
| BaseNumPorts       | The number of base ports of the component or subcomponent.                                                |
| TotalNumPorts      | The number of ports of the component or subcomponent.                                                     |
| IpAddress          | The IP address of the component or subcomponent.                                                          |
| RunningSoftwareVer | The software version.                                                                                     |

## Renumbering stack switch units using EDM

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

### Important:

#### 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.

The following table outlines the parameters for the **Stack Numbering** tab.

**Table 127: Variable definitions**

| Variable            | Value                                                                       |
|---------------------|-----------------------------------------------------------------------------|
| Current Unit Number | Indicates the current switch numbering sequence.                            |
| Descr               | Provides a description of hardware included with the selected stack switch. |
| New Unit Number     | Specifies the updated switch numbering sequence.                            |

## Variable definitions

Use the information in the following table to change the unit numbers of switches in a stack.

---

## Displaying the Ports dialog box

Port configuration tasks are performed in Enterprise Device Manager on the Port screen.

To open the Port screen:

### Procedure steps

1. In the **Device Physical View** double-click the port. Multiple ports can be edited by selecting ports with the Control (CTRL) key depressed. Or From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Ports**.

#### \* Note:

The presentation of the Port screen differs when one port is selected or multiple ports are selected. This difference is mainly in presentation although some options are not be available when multiple ports are selected. These exceptions are noted in their descriptions.

The following sections describe some of the tabs on the Port screen:

- [Displaying port status](#) on page 230
- [Viewing VLAN port properties](#) on page 233
- [Viewing the PoE power settings](#) on page 234
- [Displaying the LACP tab](#) on page 235
- [Viewing VLACP properties](#) on page 237
- [Configuring rate limiting for a single port](#) on page 238
- [Testing port cables](#) on page 239

## Displaying port status

The Interface tab shows the basic configuration and status of a port.

To open the Interface tab:

### Procedure steps

1. In the **Device Physical View** double-click the port. Multiple ports can be edited by selecting ports with the Control (CTRL) key depressed. Or From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.

3. From the Chassis tree, double-click **Ports**.
4. Select the **Interface** tab.
5. Click **Apply** after making any changes.

The following table outlines the parameters for the **Interface** tab.

**Table 128: Variable definitions**

| Variable    | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index       | A unique value assigned to each interface. The value ranges between 1 and 128 standalone. On stack, the index value of the first port of the second unit is 129. The maximum value is 512.                                                                                                                                                                                                                                                                                                                                                            |
| Name        | Use this field to enter an optional name for the port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Descr       | The type of switch and number of ports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 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 | <p>The current administrative state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• up</li> <li>• down</li> </ul> <p>When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.</p>                                                                                                |
| OperStatus  | <p>The current operational state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• up</li> <li>• down</li> <li>• testing</li> </ul> <p>If AdminStatus is up, then OperStatus is also up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus is also down. It remains 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.</p> |
| 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.                                                                                                                                                                                                                                                                                                                             |

| Variable                       | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LinkTrap                       | Indicates whether linkUp/linkDown traps are generated for this interface. By default, this object has the value enabled for interfaces that do not operate on top of any other interface (as defined in the ifStackTable).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| AutoNegotiate                  | Indicates whether this port is enabled for autonegotiation or not.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| AdminDuplex                    | Sets the administrative duplex mode of the port (half or full).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| OperDuplex                     | Shows the current administrative duplex mode of the port (half or full).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| AdminSpeed                     | Set the port speed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| OperSpeed                      | The current operating speed of the port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| AutoNegotiation Capability     | <p>Specifies the port speed and duplex capabilities that hardware can actually support on a port, and which can be advertised by the port using auto-negotiation. Bit 7 tells if a port supports pause frame capabilities (for full-duplex links) as a part of the advertisement.</p> <ul style="list-style-type: none"> <li>bit 0 - 10 half duplex advertisements</li> <li>bit 1 - 10 full duplex advertisements</li> <li>bit 2 - 100 half duplex advertisements</li> <li>bit 3 - 100 full duplex advertisements</li> <li>bit 4 - 1000 half duplex advertisements</li> <li>bit 5 - 1000 full duplex advertisements</li> <li>bit 6 - PAUSE frame support advertisements</li> <li>bit 7 - Asymmetric PAUSE frame support advertisements</li> </ul> <p>If auto-negotiation is not supported by the port hardware, then all bits reflect a value of zero.</p> |
| AutoNegotiation Advertisements | <p>Specifies the port speed and duplex abilities to be advertised during link negotiation.</p> <ul style="list-style-type: none"> <li>• 10Half: 10 half duplex advertised</li> <li>• 10Full: 10 full duplex advertised</li> <li>• 100Half: 100 half duplex advertised</li> <li>• 100Full: 100 full duplex advertised</li> <li>• 1000Half: 1000 half duplex advertised</li> <li>• 1000Full: 1000 full duplex advertised</li> <li>• PauseFrame: PAUSE frame support advertised.</li> <li>• AsymPauseFrame: Asymmetric PAUSE frame support advertised.</li> </ul> <p>The abilities specified in this object are only used when auto-negotiation is enabled on the port. If all bits in this object are</p>                                                                                                                                                    |



| Variable             | Value                                                                                                                              |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------|
|                      | disabled, and auto-negotiation is enabled on the port, then the physical link process on the port is disabled.                     |
| WanMode              | Set the area network type for a 10 GE port. <ul style="list-style-type: none"> <li>• none</li> <li>• wan</li> <li>• lan</li> </ul> |
| MltId                | The multilink trunk to which the port is assigned (if any).                                                                        |
| IsPortShared         | Displays if the selected port is a shared port or not.                                                                             |
| PortActive Component | Displays the active component of shared ports.                                                                                     |

## Viewing VLAN port properties

To view the VLAN tab:

### Procedure steps

1. In the **Device Physical View** double-click the port. Multiple ports can be edited by selecting ports with the Control (CTRL) key depressed. Or From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Ports**.
4. Select the **VLAN** tab.

The following table outlines the parameters for the **VLAN** tab.

**Table 129: Variable definitions**

| Variable      | Value                                                                                                                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VlanIds       | Specifies the IDs of the VLANs.                                                                                                                                                                                                                                                                      |
| DefaultVlanId | The VLAN ID assigned to untagged frames received on a trunk port.                                                                                                                                                                                                                                    |
| PortPriority  | Specifies the port priority value from the list as a value between 0 and 7.                                                                                                                                                                                                                          |
| Tagging       | Indicates the type of VLAN port. A trunk port can be a member of more than one VLAN. An access port can be a member of only VLAN, if no membership conflict exists. There are four types of VLAN port: <ul style="list-style-type: none"> <li>• tagAll(trunk)</li> <li>• untagAll(access)</li> </ul> |

| Variable | Value                                                                                    |
|----------|------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• tagPvidOnly</li> <li>• untagPvidOnly</li> </ul> |

For more information on the VLAN tab, see *Avaya Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and Multi-Link Trunking* (NN47200-502).

## Viewing the PoE power settings

The PoE tab enables the configuration of the PoE power settings for a port in the Avaya Ethernet Routing Switch 5520. This tab is not displayed for units other than the 5520.

To open the PoE tab:

### Procedure steps

1. In the **Device Physical View** double-click the port. Multiple ports can be edited by selecting ports with the Control (CTRL) key depressed. Or From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Ports**.
4. Select the **PoE** tab.


#### \* Note:

The **PoE** tab is for setting Power over Ethernet (PoE) parameters for each port. The **Power Supply** tab on the Chassis screen displays the status of the internal Avaya Ethernet Routing Switch power supply.

The following table outlines the parameters for the **PoE** tab.

**Table 130: Variable definitions**

| Variable         | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AdminEnable      | Enables or disables PoE on this port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Detection Status | Displays the operational status of the power-device detecting mode on the specified port: <ul style="list-style-type: none"> <li>• disabled: detecting function disabled</li> <li>• searching: detecting function is enabled and the system is searching for a valid powered device on this port</li> <li>• detected: detecting function detects a valid powered device but the port is not supplying power</li> <li>• deliveringPower: detection found a valid powered device and the port is delivering power</li> <li>• fault: power-specific fault detected on port</li> </ul> |

| Variable             | Value                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <ul style="list-style-type: none"> <li>• invalidPD: detecting function found an invalid powered device</li> <li>• denyLowPriority: port disabled by management system to supply power to higher-priority ports</li> <li>• test: detecting device in test mode</li> </ul> <p> <b>Note:</b><br/>Avaya recommends against using the test operational status.</p> |
| PowerClassifications | Displays the operational status of the port PD classification.                                                                                                                                                                                                                                                                                                                                                                                 |
| PowerPriority        | Sets the power priority for the specified port to: <ul style="list-style-type: none"> <li>• critical</li> <li>• high</li> <li>• low</li> </ul>                                                                                                                                                                                                                                                                                                 |
| PowerLimit           | Enter an integer from 3 to 16 W to set the power limit for the port.                                                                                                                                                                                                                                                                                                                                                                           |
| Power Measurement    | Read only: <ul style="list-style-type: none"> <li>• Voltage: in 1/10 v.</li> <li>• Current: in 1/1000 A.</li> <li>• Power: in 1/1000 W.</li> </ul>                                                                                                                                                                                                                                                                                             |

## Displaying the LACP tab

To display the LACP tab:

### Procedure steps

1. In the **Device Physical View** double-click the port. Multiple ports can be edited by selecting ports with the Control (CTRL) key depressed. Or From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Ports**.
4. Select the **LACP** tab.

The following table outlines the parameters for the **LACP** tab.

**Table 131: Variable definitions**

| Variable              | Value                                                                                                                                                                                                                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ActorSystemPriority   | A 2-octet read-write value indicating the priority value associated with the Actor's System ID.                                                                                                                                                                                                   |
| OperEnabled           | The current operational state for the port. A value of true means the port is participating in LACP. A value of false means the port is not participating in LACP.                                                                                                                                |
| ActorAdminState       | A string of 8 bits, corresponding to the administrative values of Actor_State as transmitted by the Actor in LACPDUs.                                                                                                                                                                             |
| ActorOperState        | A string of 8 bits, corresponding to the current operational values of Actor_State as transmitted by the Actor in LACPDUs.                                                                                                                                                                        |
| AggregateOrIndividual | The current operational state of the port, either aggregate and participating in a LAG, or individual link, not participating in a LAG. Value is read-only.                                                                                                                                       |
| ActorPortPriority     | The priority value assigned to this Aggregation Port. This 16-bit value is read-write.                                                                                                                                                                                                            |
| ActorySystemID        | The identifier for the actor system, currently the MAC address of the actor system. Value is read-only.                                                                                                                                                                                           |
| ActorOperKey          | The current operational value of the Key for the Aggregation Port. This is a 16-bit read-only value.                                                                                                                                                                                              |
| SelectedAggID         | The identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because no suitable Aggregator exists for it to select. |
| AttachedAggID         | The identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.                                                                                         |
| ActorPort             | The port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the Actor_Port. This value is read-only                                                                                                                                                   |
| PartnerOperPort       | The operational port number assigned by the port's protocol partner. This value is read-only.                                                                                                                                                                                                     |

For more information on the LACP tab, see *Avaya Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and Multi-Link Trunking (NN47200-502)*.

## Viewing VLACP properties


To view the VLACP tab:


### Procedure steps

1. In the **Device Physical View** double-click the port. Multiple ports can be edited by selecting ports with the Control (CTRL) key depressed. Or From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Ports**.
4. Select the **VLACP** tab.

The following table outlines the parameters for the **VLACP** tab.

**Table 132: Variable definitions**

| Variable          | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OperEnable        | Indicates whether VLACP is operationally enabled (true) or disabled (false).<br><br> <b>Important:</b><br>VLACP is only operational when OperEnable is true and PortState is up.                                                                                                                                                                                                                                                                                                                                                                                          |
| FastPeriodicTimer | Indicates the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 400-20000 with a default of 500.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SlowperiodicTimer | Indicates the number of milliseconds between periodic transmissions using long timeouts. Values range from 10000-30000 with a default of 30000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timeout           | Indicates whether the timeout control value is a short or long timeout.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| TimeoutScale      | Indicates the scale value used to calculate timeout from periodic time. Values range from 1–10. The default is 3.<br>With VLACP, a short interval exists between a port transmitting a VLACPDU and the partner port receiving the same VLACPDU. If the timeout-scale is set to 1, the port timeout value does not take into account the normal travel time of the VLACPDU. The port expects to receive a VLACPDU at the same moment the partner port sends it. Therefore, the delayed VLACPDU results in the link being blocked, and then enabled again when the packet arrives. Avaya recommends that you set the timeout scale to a value larger than 1. |
| EtherType         | Indicates VLACP protocol identification. The value can be entered as a numerical value ranging from 33025–33279 or a hexadecimal equivalent (8101–81ff). The default is 8103. Use                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Variable        | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | the prefix 0x to type a hexadecimal value in the dialog box. Only hexadecimal values display in the EtherType column of the VLACP work area.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| EtherMacAddress | Indicates the MAC address of the switch or stack to which this port is sending VLACPDUs. This value cannot be configured as a multicast MAC. The default value is 00:00:00:00:00:00. VLACP uses only the multicast MAC address configured when VLACP is enabled globally. This is the Layer 2 destination address used for the VLACPDUs. The port-specific EtherMACAddress specifies the MAC address of the switch or stack to which this port is sending VLACPDUs. If you do not type a value for the EtherMACAddress, the first VLACP-enabled switch that receives the PDUs from a sending port becomes the intended recipient and processes the PDUs. If you want an intermediate switch to drop VLACP packets, configure EtherMACAddress with the desired destination MAC address. With EtherMACAddress configured, the intermediate switches do not misinterpret the VLACP packets. |
| PortState       | Indicates whether the VLACP port state is up or down.<br><br> <b>Important:</b><br>VLACP is only operational when OperEnable is true and PortState is up.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

For more information on the VLACP tab, see *Avaya Ethernet Routing Switch 5000 Series Configuration — VLANs, Spanning Tree, and Multi-Link Trunking* (NN47200-502).

## Configuring rate limiting for a single port

You can use the Rate Limit tab to configure the Rate Limiting for a single port.

To open the Rate Limit tab:

### Procedure steps

1. In the **Device Physical View** double-click the port. Multiple ports can be edited by selecting ports with the Control (CTRL) key depressed. Or From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Ports**.
4. Select the **Rate Limit** tab.

The following table outlines the parameters for the **Rate Limit** tab.

**Table 133: Variable definitions**

| Variable    | Value                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------|
| TrafficType | Specifies the two types of traffic that can be set with rate limiting: broadcast and multicast.                                |
| AllowedRate | Sets the rate limiting percentage. The available range is from 0% (none) to 10%.                                               |
| Enable      | Enables and disables rate limiting on the port for the specified traffic type. Options are true (enabled) or false (disabled). |

## Testing port cables

The 5000 Series switch is equipped with a Time Domain Reflectometer (TDR). The TDR provides a diagnostic capability to test connected cables for defects (such as short pin and pin open). Use the TDR tab to initiate cable diagnostic tests on attached cables.

The cable diagnostic tests only apply to Ethernet copper ports; fiber ports cannot be tested. You can initiate a test on multiple ports at the same time.

When you test a cable with the TDR, if the cable has a 10/100 MB/s link, the link is broken during the test and restored only when the test is complete. Use of the TDR does not affect 1 GB/s links.

### \* Note:

The accuracy margin of cable length diagnosis is between three to five meters. Avaya suggests the shortest cable for length information be five meters long.

To initiate a TDR test:

### Procedure steps

1. In the **Device Physical View** double-click the port. Multiple ports can be edited by selecting ports with the Control (CTRL) key depressed. Or From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Ports**.
4. Select the **TDR** tab.
5. Select the **StartTest** option. (If multiple ports are selected, select **true** from the **StartTest** field for each port that you want to test.)
6. Click **Apply**.

The following table outlines the parameters for the **TDR** tab.

**Table 134: Variable definitions**

| Variable    | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StartTest   | Enables the TDR test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| TestDone    | Indicates whether a TDR test is complete.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| CableStatus | <p>Status of the cable as a whole. The status of a cable is, in a sense, a summation of the status of its pairs. If all the pairs are normal, the cable is normal. If the cable consists of zero or more normal pairs and one or more open pairs, the cable is considered open. If the cable consists of shorted pairs and normal pairs, it is considered shorted. Any combination of open and shorted pairs is considered simply failed.</p> <ul style="list-style-type: none"> <li>• cableFail</li> <li>• cableNormal</li> <li>• cableOpen</li> <li>• cableShorted</li> <li>• cableNotApplicable</li> <li>• cableUntested</li> </ul> |
| Pair1Status | <p>The status of a single pair in the cable:</p> <ul style="list-style-type: none"> <li>• pairFail</li> <li>• pairNormal</li> <li>• pairOpen</li> <li>• pairShorted</li> <li>• pairNotApplicable</li> <li>• pairNotTested</li> <li>• pairForce</li> </ul> <p><b>* Note:</b><br/>If a 10MB or 100MB link is established without autonegotiation, Pair 1 will return Forced mode. The pair length is meaningless in this case.</p>                                                                                                                                                                                                       |
| Pair1Length | Pair Length, in meters, measured by Time Domain Reflectometry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Pair2Status | The status of a single pair in the cable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Pair2Length | Pair Length, in meters, measured by Time Domain Reflectometry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Pair3Status | The status of a single pair in the cable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Pair3Length | Pair Length, in meters, measured by Time Domain Reflectometry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



| Variable      | Value                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pair4Status   | The status of a single pair in the cable.                                                                                                                                                                                                          |
| Pair4Length   | Pair Length, in meters, measured by Time Domain Reflectometry.                                                                                                                                                                                     |
| CableLength   | Length of cable in meters based on average electrical length of 4 pairs. Measurement can be done when traffic is live or not.                                                                                                                      |
| Pair1Polarity | The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.                                                                                                   |
| Pair1Swap     | The pair swap in the cable: <ul style="list-style-type: none"> <li>• normal</li> <li>• swapped</li> <li>• invalid</li> <li>• error</li> </ul> This capability is available only when the cable gigabit link is up, regardless of traffic activity. |
| Pair1Skew     | Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.                               |
| Pair2Polarity | The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.                                                                                                   |
| Pair2Swap     | The pair swap in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.                                                                                                                   |
| Pair2Skew     | Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.                               |
| Pair3Polarity | The polarity of a single pair in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.                                                                                                   |
| Pair3Swap     | The pair swap in the cable. This capability is available only when the cable gigabit link is up, regardless of traffic activity.                                                                                                                   |
| Pair3Skew     | Pair skew is measured in nanoseconds. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length.                               |
| Pair4Polarity | The polarity of a single pair in the cable.                                                                                                                                                                                                        |
| Pair4Swap     | The pair swap in the cable.                                                                                                                                                                                                                        |

| Variable  | Value                                                                                                                                                                                                                    |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pair4Skew | Differential cable pair length in meters. Skew measurement only can be performed when the cable gigabit link is up, regardless of traffic activity. A value of -1 means an error occurred when trying to get the length. |

## Displaying the Environment dialog box

The following section provides information about how to display switch environment details.

- [Viewing the switch power supply properties](#) on page 242
- [Displaying status of switch fans](#) on page 243
- [Viewing temperature information](#) on page 244

## Viewing the switch power supply properties

The Power Supply tab provides read-only information about the operating status of the switch power supplies.

The power supply parameters are slightly different for the Avaya Ethernet Routing Switch 5520, as it supports Power over Ethernet (PoE).

To view the Power Supply tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Environment**.
4. Select the **PowerSupply** tab.

The following table outlines the parameters for the **PowerSupply** tab.

**Table 135: Variable definitions**

| Variable    | Value                                                                                                                                                                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | Indicates the chassis number, power supply number, and the type of power supply.                                                                                                                                                                                               |
| OperStat    | The operational state of the power supply. Possible values include: <ul style="list-style-type: none"> <li>• other: Some other state.</li> <li>• notAvail: State not available.</li> <li>• removed: Component was removed.</li> <li>• disabled: Operation disabled.</li> </ul> |

| Variable | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• normal: State is in normal operation.</li> <li>• resetInProgress: There is a reset in progress.</li> <li>• testing: System is doing a self test.</li> <li>• warning: System is operating at a warning level.</li> <li>• nonFatalErr: System is operating at error level.</li> <li>• fatalErr: A fatal error stopped operation.</li> <li>• notConfig: A module needs to be configured. The allowable values are determined by the component type.</li> </ul> |

## Displaying status of switch fans

The Fan tab provides read-only information about the operating status of the switch fans.

To display status of switch fans:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the Chassis tree, double-click **Environment**.
4. Select the **Fan** tab.

The following table outlines the parameters for the **Fan** tab.

**Table 136: Variable definitions**

| Variable | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OperStat | <p>The operational state of the fan. Values include:</p> <ul style="list-style-type: none"> <li>• other: Some other state.</li> <li>• notAvail: This state is not available.</li> <li>• removed: Fan was removed.</li> <li>• disabled: Fan is disabled.</li> <li>• normal: Fan is operating in normal operation.</li> <li>• resetInProgress: A reset of the fan is in progress.</li> <li>• testing: Fan is doing a self test.</li> <li>• warning: Fan is operating at a warning level.</li> <li>• nonFatalErr: Fan is operating at error level.</li> </ul> |

| Variable | Value                                                                                                                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"><li>• fatalErr: An error stopped the fan operation</li><li>• notConfig: Fan needs to be configured. The allowable values are determined by the component type.</li></ul> |

## Viewing temperature information

The Temperature tab provides read-only information about the temperature of the switch.

To view the Temperature tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Chassis**.
3. From the **Chassis** tree, double-click **Environment**.
4. Select the **Temperature** tab.

A report of the temperature settings of the switch appears in the Environment window.

5. Click the **Refresh** tab to update the data.

---

## Avaya Energy Saver configuration using Enterprise Device Manager

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

### Navigation:

- [Global AES configuration](#) on page 244
- [AES schedule configuration](#) on page 248
- [Port-based AES configuration](#) on page 250
- [Viewing AES information using EDM](#) on page 252

---

## Global AES configuration

Use the information in this section to configure AES for an single switch or a stack.

## Navigation

- [Enabling global AES](#) on page 245
- [Disabling global AES](#) on page 245
- [Enabling global AES PoE power save mode](#) on page 246
- [Disabling global AES PoE power save mode](#) on page 246
- [Enabling AES efficiency mode](#) on page 247
- [Disabling AES efficiency mode](#) on page 247

## Enabling global AES

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. Click the **EnergySaverEnabled** box.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

The following table outlines the parameters of the **Energy Saver Globals** tab.

**Table 137: Variable definitions**

| 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

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. Click the **EnergySaverEnabled** 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

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.
  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. Click the **PoePowerSavingEnabled** 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

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. Click the **PoePowerSavingEnabled** box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

## Enabling AES efficiency mode

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

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. Click the **EfficiencyModeEnabled** box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

---

## AES schedule configuration

Use the information in this section to configure a time interval for the switch to enter lower power states.

### Navigation

- [Configuring the AES schedule on time](#) on page 248
- [Configuring the AES schedule off time](#) on page 249
- [Modifying an AES schedule on and off time status](#) on page 250

### Configuring the AES schedule on time

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, click a button in the **ScheduleDay** section.



6. To choose an hour of the day for the AES schedule on time, type a value in the **ScheduleHour** box.
7. To choose a portion of an hour for the AES schedule on time, type a value in the **ScheduleMinute** box.
8. To configure the selected day, hour, and minutes as the AES schedule on time, click the **activate** button in the ScheduleAction section.

Activate is selected by default.

9. Click **Insert**.

The following table describes the fields of **Insert Energy Saver Schedule** window.

**Table 138: Variable definitions**

| 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

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 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** box.
7. To choose a portion of an hour for the AES schedule off time, type a value in the **ScheduleMinute** box.
8. To configure the selected day, hour, and minutes as the AES schedule off time, click the **deactivate** radio button in the ScheduleAction section.

Activate is selected by default.

9. Click **Insert**.

The following table describes the fields of **Insert Energy Saver Schedule** window.

**Table 139: Variable definitions**

| Variable       | Value                                                           |
|----------------|-----------------------------------------------------------------|
| ScheduleDay    | Indicates the day on which this schedule entry takes effect.    |
| ScheduleHour   | Indicates the hour on which this schedule entry takes effect.   |
| ScheduleMinute | Indicates the Minute on which this schedule entry takes effect. |
| ScheduleAction | Activates or deactivates the energy savings.                    |

## Modifying an AES schedule on and off time status

Use 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

Configure port-based AES to enable or disable energy saving for individual ports, or all ports on a switch or stack.

## Navigation

- [Enabling AES on individual ports](#) on page 251
- [Disabling AES on individual ports](#) on page 252

## Enabling AES on individual ports

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. In the **Multiple Port Configuration** area, click the **Switch/Stack/Ports** elipsis (...).
5. Click a port or ports, or click **All**.
6. Click **Ok**.

The portlist appears in the **Switch/Stack/Ports** box.

7. In the **Multiple Port Configuration** area double-click the cell under **EnergySaverEnabled**.

A downward arrow appears.

8. Click the arrow.

A list appears.

9. Click **true**.
10. Click **Apply Selection**.
11. On the toolbar, click **Apply**.
12. Repeat steps 4 to 11 to enable AES for additional ports as required.
13. Click **Apply**.
14. On the toolbar, you can click **Refresh** to update the work area data display.

The following table describes the fields of the **Ports** tab.

**Table 140: Variable definitions**

| Field | Description         |
|-------|---------------------|
| Port  | Indicates the port. |

| Field              | Description                                                               |
|--------------------|---------------------------------------------------------------------------|
| EnergySaverEnabled | Indicates whether the Avaya Energy Saver feature is enabled for the port. |

## Disabling AES on individual ports

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. In the **Multiple Port Configuration** area, click the **Switch/Stack/Ports** elipsis (...).
5. Click a port or ports, or click **All**.
6. Click **Ok**.  
The portlist appears in the **Switch/Stack/Ports** box.
7. In the **Multiple Port Configuration** area double-click the cell under **EnergySaverEnabled**.  
A downward arrow appears.
8. Click the arrow.  
A list appears.
9. Click **false**.
10. Click **Apply Selection**.
11. On the toolbar, click **Apply**.
12. Repeat steps 4 to 11 to disable AES for additional ports as required.
13. Click **Apply**.
14. 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.

Use the data in this table to help you understand the displayed AES information.

**Table 141: Variable definitions**

| VariableValue      | Value                                                         |
|--------------------|---------------------------------------------------------------|
| UnitIndex          | Indicates the unit number of the switch.                      |
| UnitSavings(watts) | Indicates the total power capacity being saved on the switch. |
| PoeSavings(watts)  | Indicates the total PoE power being saved on the switch.      |

---

## Bridge configuration using Enterprise Device Manager

Bridge information displays the MAC Address Table for the switch.

To open the Bridge dialog box:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Bridge**.

This section provides information about the following topics:

- [Displaying bridge information](#) on page 253
- [Displaying the Transparent tab](#) on page 254
- [Displaying the Forwarding tab](#) on page 255

---

## Displaying bridge information

The Base tab displays basic Bridge information including the MAC address, type, and number of ports participating in the Bridge.

The MAC address used by the bridge must be referred to in a unique fashion; moreover, it must be the smallest MAC address (numerically) of all ports that belong to the bridge. However,

it is only required to be unique when integrated with dot1dStpPriority. A unique BridgeIdentifier is formed that is used in the Spanning Tree Protocol.

To open the Base tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Bridge**.
3. Select the **Base** tab.

The following table outlines the parameters for the **Base** tab.

**Table 142: Variable definitions**

| Variable      | Value                                                                                                                                                                                                                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BridgeAddress | MAC address of the bridge when it is referred to in a unique fashion. This address must be the smallest MAC address of all ports that belong to the bridge. However, it is has to be unique. When concatenated with dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol. |
| NumPorts      | 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.                                                                                                                    |

---

## Displaying the Transparent tab

The Transparent tab is used to view information about learned forwarding entries.

To display the Transparent tab:


### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Bridge**.
3. Select the **Transparent** tab.
4. Click **Apply** if the **AgingTime** field is modified.

The following table outlines the parameters for the **Transparent** tab.

**Table 143: Variable definitions**

| Variable             | Value                                                                                                                     |
|----------------------|---------------------------------------------------------------------------------------------------------------------------|
| LearnedEntryDiscards | Number of Forwarding Database entries learned that have been discarded due to a lack of space in the Forwarding Database. |

| Variable  | Value                                                                                                                                                                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | If this counter is increasing, 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 been occurring but is not persistent. |
| AgingTime | Timeout period in seconds for aging out dynamically learned forwarding information.<br><br> <b>Note:</b><br>The 802.1D-1990 specification recommends a default of 300 seconds.                                                |

## Displaying the Forwarding tab

The Forwarding tab displays the current state of the port, as defined by application of the Spanning Tree Protocol.

To display the Forwarding tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Bridge**.
3. Select the **Forwarding** tab.

The following table outlines the parameters for the **Forwarding** tab.

**Table 144: Variable definitions**

| Variable | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status   | The values of this fields include: <ul style="list-style-type: none"> <li>• invalid: Entry is no longer valid, but has not been removed from the table.</li> <li>• learned: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used.</li> <li>• 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.</li> <li>• mgmt(5): Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress.</li> <li>• other: None of the preceding. This includes instances where some other MIB object (not the corresponding instance of</li> </ul> |

| Variable | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if a frames addressed to the value of dot1dTpFdbAddress are being forwarded.                                                                                                                                                                                                                                                                                                                                                                 |
| Address  | A unicast MAC address for which the bridge has forwarding or filtering information.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Port     | Either the value "0" or the port number on a frame has been seen. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress<br>A value of "0" indicates that the port number has not been learned, so the bridge does have the forwarding/filtering information for this address (located 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(3). |
| Id       | The VLAN ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

---

## File System configuration using Enterprise Device Manager

This section provides information about the following topics:

- [Config/Image/Diag file tab](#) on page 256
- [ASCII file tab](#) on page 260
- [Configuring the license file](#) on page 263
- [File configuration](#) on page 264
- [Displaying Boot Image information](#) on page 266
- [Displaying the Help File Path tab](#) on page 267

---

### Config/Image/Diag file tab

This section provides information about the following topics:

- [Changing the switch software](#) on page 257
- [Storing a binary configuration file](#) on page 259
- [Retrieving a binary configuration file](#) on page 259



## Changing the switch software

The Config/Image/Diag file tab is used to change the switch software.

To open the Config/Image/Diag file tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Config/Image/Diag file** tab.

In the fields provided, specify the information necessary to perform the download process.

4. Click **Apply**.

The software download process occurs automatically after clicking **Apply**. This process erases the contents of flash memory and replaces it with the new software image. Do not interrupt the download process. Depending on network conditions, this process can take up to 10 minutes. When the download process is complete, the switch automatically resets and the new software image initiates a self-test. During the download process, the switch is not operational.

The following table outlines the parameters for the **Config/Image/Diag file** tab.

**Table 145: Variable definitions**

| Variable                 | Value                                                                                                                                                                                                                                                                            |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TftpServerIpAddressType  | The type of TFTP server on which the new software images are stored for download.                                                                                                                                                                                                |
| TftpServerIpAddress      | The IP address of the TFTP server on which the new software images are stored for download.                                                                                                                                                                                      |
| BinaryConfigFileName     | The binary configuration file currently associated with the switch. This field is used when working with configuration files and is not used when downloading a software image.                                                                                                  |
| BinaryConfigUnit Number  | The unit number of the portion of the configuration file that has to be extracted and used for the stand-alone unit configuration. If this value is 0 it is ignored. This field is used when working with configuration files and is not used when downloading a software image. |
| ImageFileName            | 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) | 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.                                                                                                                |

| Variable      | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UsbTargetUnit | This field indicates the unit number of the USB port to be used in file upload or download operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Image         | Specify if the image to download is the primary or secondary image.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Action        | <p>This group of option buttons represents the actions that are to be taken during this file system operation. The options applicable to a software download are:</p> <ul style="list-style-type: none"> <li>• dnldImg - Select this option to download 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.</li> <li>• dnldFw - Select this option to download 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.</li> <li>• dnldImgIfNewer - Select this option to download a new software image to the switch only if it is newer than the one currently in use.</li> <li>• dnldImgFromUsb - Select this option to download a new software image to the switch using the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image. This option is only available on the Avaya Ethernet Routing Switch 5530-24TFD.</li> <li>• dnldFwFromUsb - Select this option to download 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. This option is only available on the Avaya Ethernet Routing Switch 5530-24TFD or 5600 Series.</li> <li>• dnldImgNoReset - Select this option to download 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.</li> <li>• dnldFwNoReset - Select this option to download 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.</li> </ul> |
| Status        | Displays the status of the last action that occurred since the switch was last booted. The values that are displayed are:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Variable | Value                                                                                                                                                                                                                                                                                            |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• other - No action has taken place since the last boot.</li> <li>• inProgress - The selected operation is currently in progress.</li> <li>• success - The selected operation was successful.</li> <li>• fail - The selected operation failed.</li> </ul> |

## Storing a binary configuration file

To store the current binary configuration file to a TFTP server or USB storage device:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Config/Image/Diag file** tab.
4. If a default TFTP server is not already specified (or another TFTP server is to be used), enter the IP address of the TFTP server to use in the **TftpServerIpAddress** field. If the file is stored on a USB storage device, skip this step.
5. In the **BinaryConfigFilename** field enter the name to assign to the configuration file .
6. If the configuration file to be stored is part of a stack, enter the stack unit number in the **BinaryConfigUnitNumber** field. If it is a stand-alone unit, specify 0.
7. If the configuration file is saved to a USB storage device, enter the stack unit number in which the USB device is inserted in the **UsbTargetUnit** field.
8. In the **Action** field, select the **upldConfig** option to upload to a TFTP server or **upldConfigtoUsb** to upload it to a USB storage device.
9. Click **Apply**.

For more information, see [Table 145: Variable definitions](#) on page 257.

## Retrieving a binary configuration file

To retrieve a binary configuration file from a TFTP server:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Config/Image/Diag file** tab.
4. If a default TFTP server is not already specified (or another TFTP server is to be used), enter the IP address of the TFTP server to use in the

**TftpServerInetAddress** field. If the file is retrieved from a USB storage device, skip this step.

5. Enter the name of the configuration file to retrieve in the **BinaryConfigFilename** field.
6. If the configuration file to be retrieved to a member of a stack, enter the stack unit number in the **BinaryConfigUnitNumber** field. If it is a stand-alone unit, specify 0.
7. If the configuration file is retrieved from a USB storage device, enter the stack unit number in which the USB device is inserted in the **UsbTargetUnit** field.
8. In the **Action** field, select the **dnldConfig** option to download the file from a TFTP server or **dnldConfigFromUsb** to download it from a USB storage device.
9. Click **Apply**.

For more information, see [Table 145: Variable definitions](#) on page 257.

---

## ASCII file tab

This section provides information about the following topics:

- [Downloading an ASCII configuration file](#) on page 260
- [Storing the current ASCII configuration](#) on page 262
- [Retrieving an ASCII configuration file](#) on page 262

## Downloading an ASCII configuration file

This feature is enabled through Enterprise Device Manager by using the File System screen.

To enable the automatic downloading of a configuration file:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **AsciiConfigFile** tab.
4. Type the IP address of the desired TFTP server in the **TftpServerInetAddress** field.
5. Type the name of the configuration file to be used in the **AsciiConfigFilename** field.
6. From the **AsciiConfigAutoDownload** field, select the option button that represents how the configuration file is to be downloaded. The options are:
  - disabled - Automatic downloading is disabled.

- useBootp - Use BootP to obtain the settings needed to connect to the TFTP server that contains the configuration file. Using this option overrides the value in the **LoadServerAddr** field.
- useConfig - Use the TFTP settings on the screen to connect to the TFTP server.

7. Click **Apply**.

The following table outlines the parameters for the **Ascii Config File** tab.

**Table 146: Variable definitions**

| Variable                   | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TftpServerInetAddressType  | Specifies the IP address of the TFTP server for all TFTP operations. If not used, then the value is 0.0.0.0. Further, if the value of s5AgTftpServerInetAddressType is not ipv4(1), then the value of this object must be 0.0.0.0.                                                                                                                                                                                                                                                                                                   |
| TftpServerInetAddress      | This object indicates the type of address stored in the related object s5AgSysTftpServerInetAddress.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| AsciiConfigFilename        | Specifies the name of the ascii configuration file that is downloaded/uploaded either at boot time when the s5AgSysAsciiConfigAutoDownload object is set to useConfig(3), or when the s5AgSysAsciiConfigManualDownloadobject is set to downloadNow(4) or downloadFromUsb(5). When not used, the value is a zero length string.                                                                                                                                                                                                       |
| UsbTargetUnit              | Indicates the unit number of the USB port to be used in file upload/download operations                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| AsciiConfigAutoDownload    | Indicates whether an ASCII configuration file should be downloaded at boot time. The file can be downloaded using either the configured filename and TFTP server address, or a BOOTP server can be used to determine the filename and TFTP server address.                                                                                                                                                                                                                                                                           |
| AsciiConfigAutoDidStatus   | Indicates the status of the last automatic ASCII configuration file download at boot time. If no automatic download at boot time has been attempted, the value returned is failed.                                                                                                                                                                                                                                                                                                                                                   |
| AsciiConfigManualDownload  | Indicates the last manual attempt to download an ASCII configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| AsciiConfigManualDidStatus | Indicates the status of the last manual attempt to download an ASCII configuration file. The value of this object when retrieved can be either passed(1), inProgress(2), or failed(3). Setting this object to downloadNow(4) initiates a manual ASCII configuration file download from a TFTP server. Setting this object to downloadFromUsb(5) initials a manual ASCII configuration file download from a USB flash dongle. If no attempt has been made to manually download a configuration file, the value returned is failed(3). |

| Variable                     | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Applications                 | Specifies the application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| AsciiConfigManual Upload     | Indicates the the last manual attempt to upload an ASCII configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| AsciiConfigManual UpldStatus | Indicates the status of the last manual attempt to upload an ASCII configuration file. The value of this object when retrieved can be either passed(1), inProgress(2), or failed(3). Setting this object to uploadNow(4) initiates a manual ASCII configuration file upload to a TFTP server. Setting this object to uploadToUsb(5) initiates a manual ASCII configuration file upload to a USB flash dongle. If no attempt has been made to manually upload a configuration file, the value returned is failed(3)." ::= { s5AgentSystem 19 } |

## Storing the current ASCII configuration

To store the current ASCII switch configuration file to a TFTP server or USB storage device:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Ascii Config File** tab.
4. In the **TftpServerInetAddress** box type the IP address of the desired TFTP server.
5. In the **AsciiConfigFilename** box type the name of the configuration file.
6. To save the configuration file to a USB storage device, select 9 if the device is a standalone or 1-8 if the device is a stack.
7. In the **AsciiConfigManualUpload** field select **Upload Now** to transfer the file to a TFTP server or **UploadToUsb** to transfer the file to a USB mass storage device.
8. Click Apply.
9. Check the **AsciiConfigManualUpload** field for the file transfer status. If the status of the file upload is `InProgress` , wait for up to two minutes and then click **Refresh** to see the new status. The file upload is complete when the status displays either `Passed` or `Failed` .

For more information, see [Table 146: Variable definitions](#) on page 261.

## Retrieving an ASCII configuration file

To retrieve an ASCII configuration file from a TFTP server or USB storage device:

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Ascii Config File** tab.
4. In the **TftpServerInetAddress** box type the IP address of the desired TFTP server if you are retrieving the configuration file from a TFTP server.
5. If you retrieve the configuration file from a USB storage device, select 9 if the device is a stand-alone or 1-8 if the device is a stack.
6. Select **downloadNow** in the **AsciiConfigManualDownload** field to transfer the file from a TFTP server or **downloadFromUsb** to transfer the file from a USB mass storage device.
7. Click **Apply**.
8. Check the **AsciiConfigManualDidStatus** field for the file transfer status. If the status of the file upload is `InProgress` , wait for up to two minutes and then click **Refresh** to see any new status applied to the upload. The file upload is complete when the status displays either `Passed` or `Failed` .

For more information, see [Table 146: Variable definitions](#) on page 261.

---

## Configuring the license file

To configure the license file:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **License File** tab.
4. In the **TftpServerInetAddressType** field, select the address type, IPv4 or IPv6.
5. In the **TftpServerInetAddress** field, enter the TFTP server address in the format selected in the previous step.
6. In the **LicenseFileName** field, enter the software license filename for the TFTP server.
7. In the **UsbTargetUnit** field, select the target location using an integer ranging 0-9. 0 specifies TFTP retrieval. 1-8 are used to specify USB in a stack unit. 9 is used to specify a standalone unit.
8. In the **LicenseFileAction** field, select `dnldLicense`.
9. Click **Apply**.
10. Click **Refresh**. The **LicenceFileStatus** field displays the file copy progress. After the file copy completes, a warning message appears prompting you to reboot the switch and activate the license.

11. To reboot the switch, choose Edit, Chassis
12. Under the System tab, select the reboot option and click Apply.

The following table outlines the parameters for the **License File** tab.

**Table 147: Variable definitions**

| Variable                  | Value                                                                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TftpServerInetAddressType | Specifies the IP address of the TFTP server for all TFTP operations. If not used, then the value is 0.0.0.0. Further, if the value of s5AgTftpServerInetAddressType is not ipv4(1), then the value of this object must be 0.0.0.0.                    |
| TftpServerInetAddress     | Specifies the type of address of the TFTP server for all TFTP operations as IPv4 or IPv6.                                                                                                                                                             |
| LicenseFileName           | Specifies the name of the license file.                                                                                                                                                                                                               |
| UsbTargetUnt              | Specifies the USB target location. <ul style="list-style-type: none"> <li>• 1–8 specifies that the USP target unit is in the stack.</li> <li>• 9 specifies that the USB target is a standalone unit.</li> <li>• 0 specifies a TFTP server.</li> </ul> |
| LicenseFileAction         | Specifies the license file action. Only dnld license is supported.                                                                                                                                                                                    |
| LicenseFileStatus         | Displays the file copy process.                                                                                                                                                                                                                       |
| RemoveLicense             | Removes the license from a unit.                                                                                                                                                                                                                      |

---

## File configuration

Enterprise Device Manager provides tools for the storage and retrieval of configuration files.

This section provides information about the following topics:

- [Saving the current configuration](#) on page 264
- [Enabling autosave](#) on page 265
- [Disabling autosave](#) on page 266

### 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 Save Configuration tab.

To save the current configuration:



## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Config/Image/Diag file** tab.
4. Choose the Save Configuration tab.

The Save Configuration tab appears.

**\* Note:**

The shared graphic was removed in accordance with the NTDA for cloning of documents. The graphic that was removed was Edit\_FileSystem\_Save\_Config.png

5. In the **Action** field, choose **copyConfigToNvram**.
6. Click **Apply**.
7. Click Refresh The Status field displays the file copy progress.

The following table outlines the parameters for the **Save Configuration** tab.

**Table 148: Variable definitions**

| Variable               | Value                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| AutosaveToNvramEnabled | Controls whether autosaving to NVRAM is enabled. Autosaving normally occurs periodically in a background task if any configuration changes have been made |
| Action                 | Specifies where the current configuration file is saved. Only copyConfigToNvram is supported.                                                             |
| Status                 |                                                                                                                                                           |

## Enabling autosave

To enable autosave:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Save Configuration** tab.
4. Select the **AutoSaveToNvramEnabled** check box.
5. Click **Apply**.

For more information, see [Table 148: Variable definitions](#) on page 265.

## Disabling autosave

To disable autosave:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Save Configuration** tab.
4. Deselect the **AutoSaveToNvramEnabled** check box.
5. Click **Apply**.

For more information, see [Table 148: Variable definitions](#) on page 265.

---

## Displaying Boot Image information

You can view boot image information with the Boot Image tab.

To see the version of the primary and secondary boot images on your system:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Boot Image** tab.
4. Click **Refresh** to renew the information.

The following table outlines the parameters for the **Boot Image** tab.

**Table 149: Variable definitions**

| Variable                                 | Value                                                                                                                                |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Chassis <1 to 8> Primary Image version   | Displays the version number of the primary boot image.                                                                               |
| Chassis <1 to 8> Secondary Image version | Displays the version number of the secondary boot image. This line is blank if the switch does not have a secondary image in memory. |
| Chassis <1 to 8> Running Image version   | Displays the version number of the boot image currently running.                                                                     |

---

## Displaying the Help File Path tab

To open the Help File Path tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **File System**.
3. Select the **Help File Path** tab.

---

## ADAC Configuration using Enterprise Device Manager

This section provides information about the following topics:

- [Displaying the ADAC tab](#) on page 267
- [Displaying the ADAC MAC Ranges tab](#) on page 268
- [Displaying the ADAC Ports tab](#) on page 269

---

## Displaying the ADAC tab


To open the ADAC tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **ADAC**.
3. Select the **ADAC** tab.

The following table outlines the parameters of the **ADAC** tab.

**Table 150: Variable definitions**

| Variable      | Value                                                                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OperEnable    | Indicates ADAC operational state: true is enabled and false is disabled.<br><br> <b>Important:</b><br>If AdminEnable is True and OperEnable is False, this indicates an error condition such as missing Uplink and Call Server ports. |
| OperatingMode | Selects the ADAC operation mode:                                                                                                                                                                                                                                                                                         |

| Variable            | Value                                                                                                                                                                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <ul style="list-style-type: none"> <li>• untaggedFramesBasic—IP Phones send untagged frames, and the Voice VLAN is not created.</li> <li>• untaggedFramesAdvanced—IP Phones send untagged frames, and the Voice VLAN is created.</li> <li>• taggedFrames—IP Phones send tagged frames.</li> </ul> |
| VoiceVlan           | Sets the Voice VLAN ID.                                                                                                                                                                                                                                                                           |
| CallServerPortList  | Selects the Call Server port. A maximum of 8 Call Server ports are supported.                                                                                                                                                                                                                     |
| UplinkPortList      | Selects the Uplink port. A maximum of 8 Uplink ports are supported.                                                                                                                                                                                                                               |
| MacAddrRangeControl | Selects a MAC address range table control option. <ul style="list-style-type: none"> <li>• none—default</li> <li>• clearTable—clears all MAC address range table entries.</li> <li>• defaultTable—replaces all MAC address range table entries to default values.</li> </ul>                      |

## Displaying the ADAC MAC Ranges tab

To open the ADAC MAC Ranges tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **ADAC**.
3. Select the **ADAC MAC Ranges** tab.

The following table outlines the parameters of the **ADAC MAC Ranges** tab.

**Table 151: Variable definitions**

| Variable                 | Value                                                      |
|--------------------------|------------------------------------------------------------|
| MacAddrRangeLowEndIndex  | The MAC address for the low end of the MAC address range.  |
| MacAddrRangeHighEndIndex | The MAC address for the high end of the MAC address range. |

## Displaying the ADAC Ports tab


To open the ADAC Ports tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **ADAC**.
3. Select the **ADAC Portss** tab.

The following table outlines the parameters of the **ADAC Ports** tab.

**Table 152: Variable definitions**

| Variable            | Value                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index               | Indicates the switch position in a stack and the port number. The default value for a standalone switch is 1.                                                                                                                                                                                                                                                                       |
| AdminEnable         | Indicates whether ADAC is enabled (true) or disabled (false) for the port.                                                                                                                                                                                                                                                                                                          |
| OperEnable          | Indicates whether the port ADAC operational state is true (enabled) or false (disabled). This is a read-only cell.<br><br> <b>Important:</b><br>If OperEnable is false and AdminEnable is true, ADAC is disabled. This can occur if you reach the maximum number of devices supported on a port. |
| ConfigStatus        | Indicates the ADAC status for the port. <ul style="list-style-type: none"> <li>• configApplied—the ADAC configuration is applied to the port.</li> <li>• configNotApplied—the ADAC configuration is not applied to the port.</li> <li>•</li> </ul> This is a read-only cell.                                                                                                        |
| TaggedFramesPvid    | Indicates the unique Port VLAN identifier (PVID). Values range from 0–4094. A value of 0 indicates that Auto-Configuration cannot change the PVID for the port.                                                                                                                                                                                                                     |
| TaggedFramesTagging | Indicates the tagging value that Auto-Configuration applies to a port that has ADAC enabled and has tagged frames selected as the operating mode. <ul style="list-style-type: none"> <li>• tagAll—tagging is enabled on all frames</li> <li>• tagPvidOnly—tagging is enabled on frames with a PVID that matches the PVID of this port</li> </ul>                                    |

| Variable            | Value                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <ul style="list-style-type: none"> <li>• untagPvidOnly—tagging is disabled on frames with a PVID that matches the PVID of this port</li> <li>• noChange—accepts frames without change</li> </ul>                                                                                                                                                |
| AdacPortType        | Indicates how ADAC classifies the port: <ul style="list-style-type: none"> <li>• telephony—autodetection is enabled for the port</li> <li>• callServer—the port is configured as a Call Server</li> <li>• uplink—the port is configured as an Uplink</li> <li>• other—the port is not classified as telephony, callServer, or uplink</li> </ul> |
| MacDetectionEnable  | Indicates whether Autodetection of Avaya IP Phones, based on MAC address is enabled (true) or disabled (false) on the interface. <p><b>!</b> Important:</p> You cannot configure MacDetectionEnable to false if no other supported detection mechanism is enabled on the port.                                                                  |
| LldpDetectionEnable | Indicates whether Autodetection of Avaya IP Phones, based on 802.1ab is enabled (true) or disabled (false) on the interface. <p><b>!</b> Important:</p> You cannot configure LldpDetectionEnable to false if no other supported detection mechanism is enabled on the port.                                                                     |

---

## Topology configuration using Enterprise Device Manager

This section describes topology diagnostic information available in Enterprise Device Manager through the following tabs:

- [Viewing topology information](#) on page 270
- [Viewing topology table information](#) on page 271

---

### Viewing topology information

To view topology information:

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.

3. From the Diagnostics tree, double-click **Topology**.
4. Select the **Topology** tab.

The following table outlines the parameters of the **Topology** tab.

**Table 153: Variable definitions**

| Variable  | Value                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IpAddr    | The IP address of the device.                                                                                                                                                                                                          |
| Status    | Whether Avaya topology is on (topOn) or off (topOff) for the device. The default value is topOn.                                                                                                                                       |
| NmmLstChg | 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, then the value is zero. |
| NmmMaxNum | The maximum number of entries in the NMM topology table.                                                                                                                                                                               |
| NmmCurNum | The current number of entries in the NMM topology table.                                                                                                                                                                               |

---

## Viewing topology table information

To view more topology information:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **Topology**.
4. Select the **Topology Table** tab.

The following table outlines the parameters of the **Topology Table** tab.

**Table 154: Variable definitions**

| Variable          | Value                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------------|
| Slot              | The slot number in the chassis in which the topology message was received.                        |
| Port              | The port on which the topology message was received.                                              |
| IpAddr            | The IP address of the sender of the topology message.                                             |
| SegId (Slot/Port) | The segment identifier, slot , and port number from where the autotopology packets were received. |
| MacAddr           | The MAC address of the sender of the topology message.                                            |
| ChassisType       | The chassis type of the device that sent the topology message.                                    |

| Variable | Value                                                                                                                                                                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BkplType | 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 | The current state of the sender of the topology message. The choices are: <ul style="list-style-type: none"> <li>• topChanged: Topology information has recently changed.</li> <li>• heartbeat: Topology information is unchanged.</li> <li>• new: The sending agent is in a new state.</li> </ul> |

---

## System Log configuration using Enterprise Device Manager

This section has information on the following:

- [Viewing system log settings](#) on page 272
- [Viewing remote system log properties](#) on page 273
- [Viewing system logs](#) on page 274

---

### Viewing system log settings

To view the System Log Settings tab:

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **System Log**.
4. Select the **System Log Settings** tab.

The following table outlines the parameters of the **System Log Settings** tab.

**Table 155: Variable definitions**

| Variable         | Value                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------|
| Operation        | Enables (on) or disables (off) the system log.                                                                    |
| BufferFullAction | Specifies the action for the system to take when the buffer space allocated for system log messages is exhausted. |



| Variable            | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <ul style="list-style-type: none"> <li>• overwrite—previously logged messages are overwritten</li> <li>• latch—halts the saving of system log messages until overwrite is selected, or buffer space is made available by other means (for example, clearing the buffer).</li> </ul>                                                                                                                                                                                                                                                                                                                                                           |
| CurSize             | Indicates the number of messages currently stored in memory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SaveTargets         | <p>Specifies the type of system messages to save in memory.</p> <ul style="list-style-type: none"> <li>• critical—only messages classified as critical are saved in memory</li> <li>• critical/serious—only messages classified as critical and serious are saved in memory</li> <li>• critical/serious/inform—only messages classified as critical, serious, and informational are saved in memory</li> <li>• none—no system log messages are saved in memory</li> </ul>                                                                                                                                                                     |
| ClearMessageBuffers | <p>Specifies the types system log messages to delete from volatile and non-volatile memory.</p> <ul style="list-style-type: none"> <li>• volCritical—only messages classified as critical are deleted from volatile memory</li> <li>• volSerious—only messages classified as serious are deleted from volatile memory</li> <li>• volInformational—only messages classified as informational are deleted from volatile memory</li> <li>• nonVolCritical—only messages classified as critical are deleted from non-volatile memory</li> <li>• nonVolSerious—only messages classified as serious are deleted from non-volatile memory</li> </ul> |

---

## Viewing remote system log properties

To view the Remote System Log tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **System Log**.
4. Select the **Remote System Log** tab.

The following table outlines the parameters of the **Remote System Log** tab.

**Table 156: Variable definitions**

| Variable                   | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RemoteSyslogAddressType    | Specifies the type of IP address of the remote system log server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| RemoteSyslogAddress        | Specifies the IP address of the remote system log server when sending system log messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SecondarySyslogAddressType | Specifies the type of IP address of the secondary remote system log server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SecondarySyslogAddresses   | Specifies the IP address of the secondary remote system log server when sending system log messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SaveTargets                | Specifies the type of system messages to send to the remote system log server. <ul style="list-style-type: none"> <li>• critical—only messages classified as critical are sent to the remote system log server</li> <li>• critical/serious—only messages classified as critical and serious are sent to the remote system log server</li> <li>• critical/serious/inform—only messages classified as critical, serious, and informational are sent to the remote system log server</li> <li>• none—no system log messages are sent to the remote system log server</li> </ul> |

---

## Viewing system logs

To view the System Logs tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **System Log**.
4. Select the **System Logs** tab.

The following table outlines the parameters of the **System Logs** tab.

**Table 157: Variable definitions**

| Variable       | Value                                                                 |
|----------------|-----------------------------------------------------------------------|
| OrigUnitNumber | Indicates the slot or unit number of the originator of a log message. |

| Variable  | Value                                                                                                                                      |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------|
| MsgTime   | Indicates the time (in one hundredths of a second) between system initialization and the appearance of a log message in the system log.    |
| MsgIndex  | Indicates a sequential number the system assigns to a log message when it enters the system log.                                           |
| MsgScr    | Indicates whether a log message was loaded from non-volatile memory at system initialization or was generated since system initialization. |
| MsgString | Indicates the log message originator and the reason the log message was generated.                                                         |

---

## LLDP configuration using Enterprise Device Manager

Use the following tabs to configure and view LLDP global and transmit properties for local and neighbor systems:

- [Configuring LLDP transmit properties](#) on page 275
- [Configuring LLDP ports](#) on page 279
- [TX Stats](#) on page 281
- [RX Stats](#) on page 282
- [Viewing LLDP local system properties](#) on page 284
- [Viewing LLDP local port properties](#) on page 286
- [Viewing LLDP management properties](#) on page 287
- [Viewing LLDP remote management properties](#) on page 288
- [Viewing unknown TLVs received](#) on page 289
- [Viewing LLDP organizationally-specific properties](#) on page 290

---

### Configuring LLDP transmit properties

With the Globals tab, you can configure LLDP transmit properties and view remote table statistics.

To configure LLDP transmit properties:

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.

3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Globals** tab.

The following table outlines the parameters of the **LLDP Globals** tab.

**Table 158: Variable definitions**

| Variable                    | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IldpMessageTxInterval       | The interval (in seconds) at which LLDP frames are transmitted on behalf of this LLDP agent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IldpMessageTxHoldMultiplier | 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: $TTL = \min(65535, (IldpMessageTxInterval * IldpMessageTxHoldMultiplier))$ For example, if the value of IldpMessageTxInterval is 30, and the value of IldpMessageTxHoldMultiplier is 4, the value 120 is encoded in the TTL field in the LLDP header.                                                                                                                                                                                                                                                                                                                            |
| IldpReinitDelay             | The IldpReinitDelay indicates the delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| IldpTxDelay                 | The IldpTxDelay 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 IldpTxDelay is set by the following formula: $1 \leq IldpTxDelay \leq (0.25 * IldpMessageTxInterval)$                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IldpNotificationInterval    | This object controls the transmission of LLDP notifications. The agent must not generate more than one IldpRemTablesChange 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 IldpRemoteSystemsData 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 IldpStatsRemTableLastChangeTime to detect any missed IldpRemTablesChange 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. |
| RemTablesLastChangeTime     | 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 IldpRemoteSystemsData objects, and all LLDP extension objects associated with remote systems. An NMS can use this object to reduce polling of the IldpRemoteSystemsData objects.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Variable             | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RemTablesInserts     | The number of times the complete set of information advertised by a particular MSAP is inserted into tables contained in IldpRemoteSystemsData and IldpExtensions 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 IldpStatsRemTablesInserts because the insert is not completed yet or in IldpStatsRemTablesDeletes, because the deletion is only a partial deletion. If the failure is the result of a lack of resources, the IldpStatsRemTablesDrops counter is incremented once. |
| RemTablesDeletes     | The number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in IldpRemoteSystemsData and IldpExtensions 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       | The number of times the complete set of information advertised by a particular MSAP can not be entered into tables contained in IldpRemoteSystemsData and IldpExtensions objects because of insufficient resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| RemTablesAgeouts     | The number of times the complete set of information advertised by a particular MSAP is deleted from tables contained in IldpRemoteSystemsData and IldpExtensions 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| FastStartRepeatCount | The number of times the fast start LLDPDU is sent during the activation of the fast start mechanism defined by LLDP-MED.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Viewing LLDP remote properties

With the Neighbor tab, you can view LLDP properties for the remote system.

To view LLDP properties for the remote system:

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Neighbor** tab.

The following table outlines the parameters of the **LLDP Neighbor** tab.

**Table 159: Variable definitions**

| Variable         | Value                                                                                                                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark         | The TimeFilter for this entry. See the TimeFilter textual convention in IETF RFC 2021 for details about TimeFilter.                                                                                                                                                                 |
| LocalPortNum     | Identifies the local port on which the remote system information is received.                                                                                                                                                                                                       |
| Index            | An 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 | The type of encoding used to identify the remote system chassis: <ul style="list-style-type: none"> <li>• chassisComponent</li> <li>• interfaceAlias</li> <li>• portComponent</li> <li>• macAddress</li> <li>• networkAddress</li> <li>• interfaceName</li> <li>• local.</li> </ul> |
| ChassisId        | 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          | Remote system name.                                                                                                                                                                                                                                                                 |
| SysDesc          | Remote system description.                                                                                                                                                                                                                                                          |
| PortIdSubtype    | The type of encoding used to identify the remote port.                                                                                                                                                                                                                              |

| Variable | Value                                                                                                                                                                                                           |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• interfaceAlias</li> <li>• portComponent</li> <li>• macAddress</li> <li>• networkAddress</li> <li>• interfaceName</li> <li>• agentCircuitId</li> <li>• local</li> </ul> |
| PortId   | Remote port ID.                                                                                                                                                                                                 |
| PortDesc | Remote port description.                                                                                                                                                                                        |

## Configuring LLDP ports

With the Port tab, you can set the optional TLVs to include in the LLDPUs transmitted by each port.

To configure LLDP ports:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Port** tab.

The following table outlines the parameters of the **LLDP Port** tab.

**Table 160: Variable definitions**

| Variable    | Value                                                                                                                                                                                                                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum     | Port number.                                                                                                                                                                                                                                                                                                                                                       |
| AdminStatus | <p>The administratively desired status of the local LLDP agent:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• rxOnly: the LLDP agent receives but does not transmit LLDP frames on this port.</li> </ul> |

| Variable           | Value                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <ul style="list-style-type: none"> <li>• txAndRx: the LLDP agent transmits and receives LLDP frames on this port.</li> <li>• disabled: the LLDP agent does not transmit or receive LLDP frames on this port. If the port receives remote systems information which is stored in other tables before AdminStatus is disabled, the information ages out.</li> </ul>                    |
| NotificationEnable | <p>Controls, for each port, whether notifications from the agent are enabled.</p> <ul style="list-style-type: none"> <li>• true: indicates that notifications are enabled</li> <li>• false: indicates that notifications are disabled.</li> </ul>                                                                                                                                    |
| TLVsTxEnable       | <p>Sets the optional Management TLVs to be included in the transmitted LLDPDUs:</p> <ul style="list-style-type: none"> <li>• portDesc: Port Description TLV</li> <li>• sysName: System Name TLV</li> <li>• sysDesc: System Description TLV</li> <li>• sysCap: System Capabilities TLV</li> </ul> <p>Note: The Local Management tab controls Management Address TLV transmission.</p> |
| VLANTxEnable(dot1) | <p>Specifies whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is included in the transmitted LLDPDUs.</p>                                                                                                                                                                                                                                                  |
| TLVsTxEnable(dot3) | <p>Sets the optional IEEE 802.3 organizationally defined TLVs to be included in the transmitted LLDPDUs:</p> <ul style="list-style-type: none"> <li>• macPhyConfigStatus: MAC/PHY configuration/status TLV</li> <li>• powerViaMDI: Power over MDI TLV</li> <li>• linkAggregation: Link Aggregation TLV</li> <li>• maxFrameSize: Maximum-frame-size TLV.</li> </ul>                   |
| CapSupported(med)  | <p>Identifies which MED system capabilities are supported on the local system.</p>                                                                                                                                                                                                                                                                                                   |
| TLVsTxEnable(med)  | <p>Sets the optional organizationally defined TLVs for MED devices to include in the transmitted LLDPDUs:</p> <ul style="list-style-type: none"> <li>• capabilities: Capabilities TLVs</li> <li>• networkPolicy: Network Policy TLVs</li> <li>• location: Emergency Communications System Location TLVs</li> </ul>                                                                   |



| Variable          | Value                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <ul style="list-style-type: none"> <li>extendedPSE: Extended PoE TLVs with PSE capabilities</li> <li>inventory: Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, and Asset ID TLVs.</li> </ul> |
| NotifyEnable(med) | A value of true enables sending the topology change traps on this port. A value of false disables sending the topology change traps on this port.                                                                                                    |

## TX Stats

This section provides information about the following topics:

- [Displaying the TX Stats tab](#) on page 281
- [Graphing LLDP transmit statistics](#) on page 282

### Displaying the TX Stats tab

With the TX Stats tab, you can view LLDP transmit statistics by port.

To open the TX Stats tab:

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **TX Stats** tab.

The following table outlines the parameters of the **LLDP TX Stats** tab.

**Table 161: Variable definitions**

| Variable    | Value                                                                          |
|-------------|--------------------------------------------------------------------------------|
| PortNum     | port number                                                                    |
| FramesTotal | the number of LLDP frames transmitted by this LLDP agent on the indicated port |

## Graphing LLDP transmit statistics

To graph LLDP transmit statistics:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **TX Stats** tab.
6. Click **Graph**. The TX Stats - Graph dialog box appears.
7. Highlight a data column to graph.
8. Click one of the graph buttons.

---

## RX Stats

This section provides information about the following topics:

- [Displaying the RX Stats tab](#) on page 282
- [Graphing LLDP receive statistics](#) on page 283

## Displaying the RX Stats tab

With the RX Stats tab, you can view LLDP receive statistics by port.

To open the RX Stats tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **RX Stats** tab.

The following table outlines the parameters of the **LLDP RX Stats** tab.

**Table 162: Variable definitions**

| Variable              | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum               | Port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FramesDiscardedTotal  | 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          | The number of invalid LLDP frames received on the port, while the LLDP agent is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| FramesTotal           | The number of valid LLDP frames received on the port, while the LLDP agent is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| TLVsDiscardedTotal    | The number of LLDP TLVs discarded for any reason.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| TLVsUnrecognizedTotal | 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 of IEEE 802.1AB-2004. An unrecognized TLV can be a basic management TLV from a later LLDP version.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| AgeoutsTotal          | This counter 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 contained in IldpRemoteSystemsData and IldpExtensions objects because the information timeliness interval has expired." This counter is similar to IldpStatsRemTablesAgeouts, except that it is on a per-port basis. This enables NMS to poll tables associated with the IldpRemoteSystemsData 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 receive statistics

To graph LLDP receive statistics:

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **RX Stats** tab.
6. Click **Graph**. The RX Stats - Graph dialog box appears.
7. Highlight a data column to graph.
8. Click one of the graph buttons.

---

## Viewing LLDP local system properties

With the Local System tab, you can view LLDP properties for the local system.

To view LLDP local system properties:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Local System** tab.

The following table outlines the parameters of the **LLDP Local System** tab.

**Table 163: Variable definitions**

| Variable         | Value                                                                                                                                                                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ChassisIdSubtype | the type of encoding used to identify the local system chassis: <ul style="list-style-type: none"> <li>• chassisComponent</li> <li>• interfaceAlias</li> <li>• portComponent</li> <li>• macAddress</li> <li>• networkAddress</li> <li>• interfaceName</li> <li>• local</li> </ul> |
| ChassisId        | chassis ID                                                                                                                                                                                                                                                                        |

| Variable        | Value                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SysName         | local system name                                                                                                                                                                                                                                                                                                                                                                             |
| SysDesc         | local system description                                                                                                                                                                                                                                                                                                                                                                      |
| SysCapSupported | identifies the system capabilities supported on the local system                                                                                                                                                                                                                                                                                                                              |
| SysCapEnabled   | identifies the system capabilities that are enabled on the local system                                                                                                                                                                                                                                                                                                                       |
| DeviceClass     | local MED device class                                                                                                                                                                                                                                                                                                                                                                        |
| HardwareRev     | the vendor-specific hardware revision string as advertised by the local device                                                                                                                                                                                                                                                                                                                |
| FirmwareRev     | the vendor-specific firmware revision string as advertised by the local device                                                                                                                                                                                                                                                                                                                |
| SoftwareRev     | the vendor-specific software revision string as advertised by the local device                                                                                                                                                                                                                                                                                                                |
| SerialNum       | the vendor-specific serial number as advertised by the local device                                                                                                                                                                                                                                                                                                                           |
| MfgName         | the vendor-specific manufacturer name as advertised by the local device                                                                                                                                                                                                                                                                                                                       |
| ModelName       | the vendor-specific model name as advertised by the local device                                                                                                                                                                                                                                                                                                                              |
| AssetID         | the vendor-specific asset tracking identifier as advertised by the local device                                                                                                                                                                                                                                                                                                               |
| DeviceType      | <p>defines the type of Power-via-MDI (Power over Ethernet) advertised by the local device:</p> <ul style="list-style-type: none"> <li>• pseDevice: indicates that the device is advertised as a Power Sourcing Entity (PSE).</li> <li>• pdDevice: indicates that the device is advertised as a Powered Device (PD)</li> <li>• none: indicates that the device does not support PoE</li> </ul> |
| PSEPowerSource  | <p>defines the type of PSE Power Source advertised by the local device:</p> <ul style="list-style-type: none"> <li>• primary: indicates that the device advertises its power source as primary</li> <li>• backup: indicates that the device advertises its power source as backup</li> </ul>                                                                                                  |
| PDPowerReq      | specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD)                                                                                                                                                                                                                                                                                                    |
| PDPowerSource   | defines the type of power source advertised as in use by the local device:                                                                                                                                                                                                                                                                                                                    |

| Variable        | Value                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <ul style="list-style-type: none"> <li>• fromPSE: indicates that the device advertises its power source as received from a PSE</li> <li>• local: indicates that the device advertises its power source as local</li> <li>• localAndPSE: indicates that the device advertises its power source as using both local and PSE power</li> </ul>                                                          |
| PDPowerPriority | defines the priority advertised as required by this PD: <ul style="list-style-type: none"> <li>• critical: indicates that the device advertises its power priority as critical, see RFC 3621</li> <li>• high: indicates that the device advertises its power priority as high, see RFC 3621</li> <li>• low: indicates that the device advertises its power priority as low, see RFC 3621</li> </ul> |

## Viewing LLDP local port properties

With the Local Port tab, you can view LLDP port properties for the local system.

To view LLDP local port properties:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Local System** tab.

The following table outlines the parameters of the **LLDP Local Port** tab.

**Table 164: Variable definitions**

| Variable      | Value                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum       | Port number.                                                                                                                                                                                 |
| PortIdSubtype | The type of port identifier encoding used in the associated PortId object. <ul style="list-style-type: none"> <li>• interfaceAlias</li> <li>• portComponent</li> <li>• macAddress</li> </ul> |

| Variable | Value                                                                                                                                                                                                             |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• networkAddress</li> <li>• interfaceName</li> <li>• agentCircuitId</li> <li>• local.</li> </ul>                                                                           |
| PortId   | The string value used to identify the port component associated with a given port in the local system.                                                                                                            |
| PortDesc | 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 management properties

With the Local Management tab, you can view LLDP management properties for the local system.

To view LLDP management properties:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Local Management** tab.

The following table outlines the parameters of the **LLDP Local Management** tab.

**Table 165: Variable definitions**

| Variable    | Value                                                                                                                                                                                                                                                                                             |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AddrSubtype | The type of management address identifier encoding used in the associated Addr object.                                                                                                                                                                                                            |
| Addr        | The string value used to identify the management address component associated with the local system. This address is used to contact the management entity.                                                                                                                                       |
| AddrLen     | 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 an iana family numbers/ |

| Variable          | Value                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | 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. <ul style="list-style-type: none"> <li>• unknown</li> <li>• ifIndex</li> <li>• systemPortNumber</li> </ul> |
| AddrIfId          | The integer value used to identify the interface number of the management address component associated with the local system.                                                                                     |
| AddrOID           | 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 | Identifies the ports on which the local system management address TLVs are transmitted in the LLPDUs.                                                                                                             |

## Viewing LLDP remote management properties

With the Neighbor Mgmt Address tab, you can view LLDP management properties for the remote system.

To open the Neighbor Mgmt Address tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Neighbor Mgmt Address** tab.

The following table outlines the parameters of the **LLDP Neighbor Mgmt Address** tab.

**Table 166: Variable definitions**

| Variable     | Value                                                                         |
|--------------|-------------------------------------------------------------------------------|
| TimeMark     | The TimeFilter for this entry.                                                |
| LocalPortNum | Identifies the local port on which the remote system information is received. |



| Variable      | Value                                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index         | An 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   | The type of encoding used in the associated Addr object.                                                                                                                                                          |
| Addr          | The management address associated with the remote system.                                                                                                                                                         |
| AddrIfSubtype | Identifies the numbering method used to define the interface number associated with the remote system. <ul style="list-style-type: none"> <li>• unknown</li> <li>• ifIndex</li> <li>• systemPortNumber</li> </ul> |
| AddrIfId      | The integer value used to identify the interface number of the management address component associated with the remote system.                                                                                    |
| AddrOID       | 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 unknown TLVs received

With the Unknown TLV tab, you can view details about unknown TLVs received on the local system.

To view the Unknown TLV tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Unknown TLV** tab.

The following table outlines the parameters of the **LLDP Unknown TLV** tab.

**Table 167: Variable definitions**

| Variable | Value                          |
|----------|--------------------------------|
| TimeMark | The TimeFilter for this entry. |

| Variable       | Value                                                                                                                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LocalPortNum   | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index          | An 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 | The value extracted from the type field of the unknown TLV.                                                                                                                                                     |
| UnknownTLVInfo | The value extracted from the value field of the unknown TLV.                                                                                                                                                    |

## Viewing LLDP organizationally-specific properties

With the Organizational Defined Info tab, you can view Organizationally-specific properties for the remote system.

To view LLDP organizationally-specific properties:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **LLDP**.
5. Select the **Organizational Defined Info** tab.

The following table outlines the parameters of the **LLDP Organizational Defined Info** tab.

**Table 168: Variable definitions**

| Variable      | Value                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark      | The TimeFilter for this entry.                                                                                                                                                                                             |
| LocalPortNum  | Identifies the local port on which the remote system information is received.                                                                                                                                              |
| Index         | An 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.            |
| OrgDefInfoOUI | The Organizationally Unique Identifier (OUI), 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. |

| Variable          | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OrgDefInfoSubtype | 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 contained in the information string.                                                                                    |
| OrgDefInfoIndex   | This object 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 IldpRemOrgDefInfoSubtype 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 IldpRemOrgDefInfoIndex will wrap between reboots. |
| OrdDefInfo        | 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 Enterprise Device Manager

You can use the LLDP Port dot1 dialog box to configure and view IEEE 802.1 LLDP information. For details, refer to the following tabs:

- [Viewing LLDP VLAN ID properties](#) on page 291
- [Viewing LLDP protocol VLAN properties](#) on page 292
- [Viewing LLDP VLAN Name properties](#) on page 293
- [Viewing LLDP protocol properties](#) on page 293
- [Viewing LLDP VLAN ID properties](#) on page 294
- [Viewing LLDP Neighbor Protocol VLAN properties](#) on page 295
- [Viewing LLDP VLAN Name properties](#) on page 296
- [Viewing LLDP Neighbor Protocol properties](#) on page 296

---

### Viewing LLDP VLAN ID properties

With the Local VLAN Id tab, you can view LLDP VLAN ID properties for the local system.

To open the Local VLAN Id tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot1**.
5. Select the **Local VLAN Id** tab.

The following table outlines the parameters of the **Port dot1 Local VLAN Id** tab.

**Table 169: Variable definitions**

| Variable | Value                                                                                 |
|----------|---------------------------------------------------------------------------------------|
| PortNum  | Port number.                                                                          |
| VlanId   | The local port VLAN ID. A value of zero is used if the system does not know the PVID. |

---

## Viewing LLDP protocol VLAN properties

With the Local Protocol VLAN tab, you can view LLDP Protocol VLAN properties for the local system.

To view LLDP protocol VLAN properties:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot1**.
5. Select the **Local Protocol VLAN** tab.

The following table outlines the parameters of the **Port dot1 Local Protocol VLAN** tab.

**Table 170: Variable definitions**

| Variable           | Value                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum            | Port number.                                                                                                                                            |
| ProtoVlanId        | 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). |
| ProtoVlanSupported | Indicates whether the local port supports port and protocol VLANs.                                                                                      |

| Variable          | Value                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------------|
| ProtoVlanEnabled  | Indicates whether the port and protocol VLANs are enabled on the local port.                                |
| ProtoVlanTxEnable | Indicates whether the corresponding local port and protocol VLAN information are transmitted from the port. |

## Viewing LLDP VLAN Name properties

With the Local VLAN Name tab, you can view LLDP VLAN Name properties for the local system.

To view the Local VLAN Name tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot1**.
5. Select the **Local VLAN Name** tab.

The following table outlines the parameters of the **Port dot1 Local VLAN Name** tab.

**Table 171: Variable definitions**

| Variable         | Value                                                                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum          | Port number.                                                                                                                                                                                                                                                            |
| VlanId           | The integer value used to identify the IEEE 802.1Q VLAN IDs with which the given port is compatible.                                                                                                                                                                    |
| VlanName         | 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 | Indicates whether the corresponding Local System VLAN name instance is transmitted from the port.                                                                                                                                                                       |

## Viewing LLDP protocol properties

With the Local Protocol tab, you can view LLDP protocol properties for the local system.

To open the Local Protocol tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot1**.
5. Select the **Local Protocol** tab.

The following table outlines the parameters of the **Port dot1 Local Protocol** tab.

**Table 172: Variable definitions**

| Variable         | Value                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------|
| PortNum          | Port number.                                                                                              |
| ProtocollIndex   | An arbitrary local integer value used by this agent to identify a particular protocol identity.           |
| ProtocollId      | The octet string value used to identify the protocols associated with the given port of the local system. |
| ProtocolTxEnable | Indicates whether the corresponding Local System Protocol Identity instance is transmitted on the port.   |

---

## Viewing LLDP VLAN ID properties

With the Neighbor VLAN Id tab, you can view LLDP VLAN ID properties for the remote system.

To view the Neighbor VLAN Id tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot1**.
5. Select the **Neighbor VLAN Id** tab.

The following table outlines the parameters of the **Port dot1 Neighbor VLAN Id** tab.

**Table 173: Variable definitions**

| Variable | Value                          |
|----------|--------------------------------|
| TimeMark | The TimeFilter for this entry. |

| Variable     | Value                                                                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LocalPortNum | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index        | An 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       | The port VLAN identifier associated with the remote system. If the remote system does not know the PVID or does not support port-based VLAN operation, the value is zero.                                       |

## Viewing LLDP Neighbor Protocol VLAN properties

With the Neighbor Protocol VLAN tab, you can view LLDP Protocol VLAN properties for the remote system.

To view the Neighbor Protocol VLAN tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot1**.
5. Select the **Neighbor Protocol VLAN** tab.

The following table outlines the parameters of the **Port dot1 Neighbor Protocol VLAN** tab.

**Table 174: Variable definitions**

| Variable          | Value                                                                                                                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark          | The TimeFilter for this entry.                                                                                                                                                                                  |
| LocalPortNum      | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index             | An 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       | 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.                                                                                                                                             |

| Variable         | Value                                                                         |
|------------------|-------------------------------------------------------------------------------|
| ProtoVlanEnabled | Indicates whether the port and protocol VLANs are enabled on the remote port. |

---

## Viewing LLDP VLAN Name properties

With the Neighbor VLAN Name tab, you can view LLDP VLAN Name properties for the remote system.

To open the Neighbor VLAN Name tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot1**.
5. Select the **Neighbor VLAN Name** tab.

The following table outlines the parameters of the **Port dot1 Neighbor VLAN Name** tab.

**Table 175: PVariable definitions**

| Variable     | Value                                                                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark     | The TimeFilter for this entry.                                                                                                                                                                                  |
| LocalPortNum | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index        | An 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       | The integer value used to identify the IEEE 802.1Q VLAN IDs with which the remote port is compatible.                                                                                                           |
| VlanName     | The VLAN name identified by the VLAN ID associated with the remote system.                                                                                                                                      |

---

## Viewing LLDP Neighbor Protocol properties

With the Neighbor Protocol tab, you can view LLDP Protocol properties for the remote system.

To view the Neighbor Protocol tab:



## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot1**.
5. Select the **Neighbor Protocol** tab.

The following table outlines the parameters of the **Port dot1 Neighbor Protocol** tab.

**Table 176: Variable definitions**

| Variable      | Value                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark      | The TimeFilter for this entry.                                                                                                                                                                                  |
| LocalPortNum  | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index         | An 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 | This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity.                                                                                          |
| ProtocolId    | Identifies the protocols associated with the remote port.                                                                                                                                                       |

---

## LLDP Port dot3 configuration using Enterprise Device Manager

You can use the LLDP Port dot3 dialog box to configure and view IEEE 802.3 LLDP information. For details, refer to the following tabs:

- [Viewing LLDP auto-negotiation properties](#) on page 298
- [Viewing LLDP PoE properties](#) on page 298
- [Viewing LLDP link aggregation properties](#) on page 299
- [Viewing LLDP maximum frame size properties](#) on page 300
- [Viewing LLDP neighbor auto-negotiation properties](#) on page 301
- [Viewing LLDP neighbor PoE properties](#) on page 301
- [Viewing LLDP neighbor link aggregation properties](#) on page 303
- [Viewing LLDP neighbor maximum frame size properties](#) on page 303

---

## Viewing LLDP auto-negotiation properties

With the Local Port Auto-negotiation tab, you can view LLDP auto-negotiation properties for the local system.

To view the Local Port Auto-negotiation tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Local Port Auto-negotiation** tab.

The following table outlines the parameters of the **Port dot3 Local Port Auto-negotiation** tab.

**Table 177: Variable definitions**

| Variable             | Value                                                                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum              | Port number.                                                                                                                                                 |
| AutoNegSupported     | Indicates whether the local port supports Auto-negotiation.                                                                                                  |
| AutoNegEnabled       | Indicates whether Auto-negotiation is enabled on the local port.                                                                                             |
| AutoNegAdvertisedCap | This object contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the local port on the system. |
| OperMauType          | A value that indicates the operational MAU type of the given port on the local system.                                                                       |

---

## Viewing LLDP PoE properties

With the Local PoE tab, you can view LLDP PoE properties for the local system.

To open the Local PoE tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.

4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Local PoE** tab.

The following table outlines the parameters of the **Port dot3 Local PoE** tab.

**Table 178: Variable definitions**

| Variable             | Value                                                                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum              | Port number.                                                                                                                                                                                                                                                   |
| PowerPortClass       | Identifies 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 | 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           | This object contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the local port: <ul style="list-style-type: none"> <li>• signal</li> <li>• spare</li> </ul>                                                                  |
| PowerClass           | This object contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the local port: <ul style="list-style-type: none"> <li>• class0</li> <li>• class1</li> <li>• class2</li> <li>• class3</li> <li>• class4</li> </ul> |

---

## Viewing LLDP link aggregation properties

With the Local Link Aggregate tab, you can view LLDP link aggregation properties for the local system.

To view the Local Link Aggregate tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.

3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Local Link Aggregate** tab.

The following table outlines the parameters of the **Port dot3 Local Link Aggregate** tab.

**Table 179: Variable definitions**

| Variable      | Value                                                                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum       | 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 maximum frame size properties

With the Local Max Frame tab, you can view LLDP maximum frame size properties for the local system.

To view the Local Max Frame tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Local Max Frame** tab.

The following table outlines the parameters of the **Port dot3 Local Max Frame** tab.

**Table 180: Variable definitions**

| Variable     | Value                           |
|--------------|---------------------------------|
| PortNum      | port number                     |
| MaxFrameSize | maximum frame size for the port |

---

## Viewing LLDP neighbor auto-negotiation properties

With the Neighbor Port Auto-Negotiation tab, you can view LLDP auto-negotiation properties for the remote system.

To view the Neighbor Port Auto-Negotiation tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Neighbor Port Auto-negotiation** tab.

The following table outlines the parameters of the **Port dot3 Neighbor Port Auto-negotiation** tab.

**Table 181: Variable definitions**

| Variable             | Value                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark             | The TimeFilter for this entry.                                                                                                                                                                                  |
| LocalPortNum         | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index                | An 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. |
| AutoNegSupported     | 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 | This object contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the remote port.                                                                 |
| OperMauType          | A value that indicates the operational MAU type of the given port on the remote system.                                                                                                                         |

---

## Viewing LLDP neighbor PoE properties

With the Neighbor PoE tab, you can view LLDP PoE properties for the remote system.

To view the Neighbor PoE tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Neighbor PoE** tab.

The following table outlines the parameters of the **Port dot3 Neighbor PoE** tab.

**Table 182: Variable definitions**

| Variable             | Value                                                                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark             | The TimeFilter for this entry.                                                                                                                                                                                                                                  |
| LocalPortNum         | Identifies the local port on which the remote system information is received.                                                                                                                                                                                   |
| Index                | An 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       | Identifies the port Class of the remote port.                                                                                                                                                                                                                   |
| PowerMDISupported    | Indicates whether MDI power is supported on the remote port.                                                                                                                                                                                                    |
| PowerMDIEnabled      | Indicates whether MDI power is enabled on the remote port.                                                                                                                                                                                                      |
| PowerPairControlable | 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           | This object contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the remote port. <ul style="list-style-type: none"> <li>• signal</li> <li>• spare</li> </ul>                                                                  |
| PowerClass           | This object contains the value of the pethPsePortPowerClassifications object (defined in IETF RFC 3621) for the remote port. <ul style="list-style-type: none"> <li>• class0</li> <li>• class1</li> <li>• class2</li> <li>• class3</li> <li>• class4</li> </ul> |

---

## Viewing LLDP neighbor link aggregation properties

With the Neighbor Link Aggregate tab, you can view LLDP link aggregation properties for the remote system.

To view the Neighbor Link Aggregate tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Neighbor Link Aggregate** tab.

The following table outlines the parameters of the **Port dot3 Neighbor Link Aggregate** tab.

**Table 183: Variable definitions**

| Variable      | Value                                                                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark      | The TimeFilter for this entry.                                                                                                                                                                                                                                                                     |
| LocalPortNum  | Identifies the local port on which the remote system information is received.                                                                                                                                                                                                                      |
| Index         | An 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 size properties

With the Neighbor Max Frame tab, you can view LLDP maximum frame size properties for the remote system.

To view the Neighbor Max Frame tab:

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port dot3**.
5. Select the **Neighbor Max Frame** tab.

The following table outlines the parameters of the **Port dot3 Neighbor Max Frame** tab.

**Table 184: Variable definitions**

| Variable     | Value                                                                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark     | The TimeFilter for this entry.                                                                                                                                                                                  |
| LocalPortNum | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index        | An 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 | Maximum Frame Size for the remote port.                                                                                                                                                                         |

---

## LLDP Port MED configuration using Enterprise Device Manager

You can use the LLDP Port med dialog box to configure and view MED LLDP information. For details, refer to the following tabs:

- [Viewing local policy properties](#) on page 305
- [Local Location](#) on page 306
- [Viewing LLDP local PoE PSE properties](#) on page 309
- [Viewing LLDP neighbor capabilities properties](#) on page 310
- [Viewing LLDP neighbor policy properties](#) on page 311
- [Viewing LLDP neighbor location properties](#) on page 312
- [Viewing LLDP neighbor PoE properties](#) on page 314
- [Viewing LLDP neighbor PoE PSE properties](#) on page 315
- [Viewing LLDP neighbor PoE PD properties](#) on page 316
- [Viewing LLDP neighbor inventory properties](#) on page 317



## Viewing local policy properties

With the Local Policy tab, you can view LLDP policy properties for the local system.

To open the Local Policy tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local Policy** tab.
6. Click **Insert**. The **Insert Local Policy** dialog box appears.
7. Enter the parameters according to the Variable definitions table.
8. Click **Insert**.

The following table outlines the parameters of the **Port MED Local Policy** tab.

**Table 185: Variable definitions**

| Variable       | Value                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum        | Port number.                                                                                                                                                                                                                                                                                                                                                                                  |
| PolicyAppType  | Voice or voice-signaling application type.                                                                                                                                                                                                                                                                                                                                                    |
| PolicyVlanID   | An 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.                                                                                                                                                                                                                                                                                                           |
| PolicyDscp     | This object 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.                                                                                                                                                                                                           |
| PolicyTagged   | A value of true indicates that the application is using a tagged VLAN. A value of false indicates that for the specific application, the device is using an untagged VLAN or does not support a port based VLAN operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance.                                                 |

---

## Local Location

This section contains information about the following topics:

- [Viewing local location properties](#) on page 306
- [Viewing coordinate-based location details](#) on page 306
- [Viewing civic address location details](#) on page 308

### Viewing local location properties

With the Local Location tab, you can view LLDP location properties for the local system.

To open the Local Location tab:

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local Location** tab.

The following table outlines the parameters of the **Port MED Local Location** tab.

**Table 186: Variable definitions**

| Variable        | Value                                                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum         | Port number.                                                                                                                                                                         |
| LocationSubtype | The location subtype advertised by the remote device: <ul style="list-style-type: none"> <li>• unknown</li> <li>• coordinateBased</li> <li>• civicAddress</li> <li>• elin</li> </ul> |
| LocationInfo    | The location information. The parsing of this information is dependent on the value LocationSubtype.                                                                                 |

### Viewing coordinate-based location details

You can select and view or configure details for coordinate-based locations listed on the Local Location tab.

To view or configure details for coordinate-based locations:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local Location** tab.
6. Select a location with the LocationSubtype listed as coordinateBased.  
The Location Detail button is activated.
7. Click the **Location Detail** button to view or configure the local detailed location information. The **Insert Local Location** dialog box appears.
8. Enter the parameters according to the Variable definitions table.
9. Click **Ok**.

The following table outlines the parameters of the **Port MED Coordinate Based Location** dialog box.

**Table 187: Variable definitions**

| Variable  | Value                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 reference datum. The format can be one of the following: <ul style="list-style-type: none"> <li>• WGS84: World Geodesic System 1984, Prime Meridian Name: Greenwich</li> <li>• NAD83/NAVD88 North American Datum 1983/ North American Vertical Datum of 1988</li> <li>• NAD83/MLLW: North American Datum 1983/ Mean Lower Low Water</li> <li>•</li> </ul> |

## Viewing civic address location details

You can select and view or configure details for civic address locations listed on the Local Location tab.

### Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

To view and configure details for civic address locations:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local Location** tab.
6. Select a location with the **LocationSubtype** listed as civicAddress  
The Location Detail button is activated.
7. Click the **Location Detail** button.  
The Civic Address Location dialog box opens.
8. Enter details and click **OK**.
9. Click **Close**.

The following table outlines the parameters of the **Port MED Civic Address Location** dialog box.

**Table 188: Variable definitions**

| Variable                    | Value                                         |
|-----------------------------|-----------------------------------------------|
| Country Code                | Country code (2 upper case letters)           |
| State                       | National subdivisions (state, canton, region) |
| County                      | County, parish, gun (JP), district (IN)       |
| City                        | City, township, shi (JP)                      |
| City District               | City division, city district, ward            |
| Block (Neighborhood, block) | Neighborhood, block                           |

| Variable                             | Value                           |
|--------------------------------------|---------------------------------|
| Street                               | Street                          |
| Leading street direction             | Leading street direction        |
| Trailing street suffix               | Trailing street suffix          |
| Street suffix                        | Street suffix                   |
| House number                         | House number                    |
| House number suffix                  | House number suffix             |
| Landmark or vanity address           | Landmark or vanity address      |
| Additional Location info             | Additional location information |
| Name (Residence and office occupant) | Residence and office occupant   |
| Postal/Zip code                      | Postal/Zip code                 |
| Building (structure)                 | Building (structure)            |
| Apartment (suite)                    | Unit number (apartment, suite)  |
| Floor                                | Floor                           |
| Room number                          | Room number                     |
| Place type                           | Office                          |
| Postal community name                | Postal community name           |
| Post office box P.O.Box              | Post office box                 |
| Additional Code                      | Additional code                 |

---

## Viewing LLDP local PoE PSE properties

With the Local PoE PSE tab, you can view LLDP PoE PSE properties for the local system.

To view the Local PoE PSE tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Local PoE PSE** tab.

The following table outlines the parameters of the **Port MED Local PoE PSE** tab.

**Table 189: Variable definitions**

| Variable              | Value                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum               | Port number.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| PSEPortPowerAvailable | This object 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: <ul style="list-style-type: none"> <li>• unknown: priority is not configured or known by the PD</li> <li>• critical: the device advertises its power priority as critical, see RFC 3621</li> <li>• high: the device advertises its power priority as high, see RFC 3621</li> <li>• low: the device advertises its power priority as low, see RFC 3621</li> </ul> |

---

## Viewing LLDP neighbor capabilities properties

With the Neighbor Capabilities tab, you can view LLDP capabilities properties for the remote system.

To view the Neighbor Capabilities tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Capabilities** tab.

The following table outlines the parameters of the **Port MED Neighbor Capabilities** tab.

**Table 190: Variable definitions**

| Variable     | Value                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------|
| TimeMark     | The TimeFilter for this entry.                                                                                      |
| LocalPortNum | Identifies the local port on which the remote system information is received.                                       |
| Index        | An arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign |

| Variable     | Value                                                                                       |
|--------------|---------------------------------------------------------------------------------------------|
|              | 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  | Remote MED device class.                                                                    |

## Viewing LLDP neighbor policy properties

With the Neighbor Policy tab, you can view LLDP policy properties for the remote system.

To view the Neighbor Policy tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Policy** tab.

The following table outlines the parameters of the **Port MED Neighbor Policy** tab.

**Table 191: Variable definitions**

| Variable     | Value                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark     | The TimeFilter for this entry.                                                                                                                                                                                                                                                                                                                                                                     |
| LocalPortNum | Identifies the local port on which the remote system information is received.                                                                                                                                                                                                                                                                                                                      |
| Index        | An 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.                                                                                                                                                                                    |
| PolicyVlanID | An 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. |

| Variable       | Value                                                                                                                                                                                                                                                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PolicyPriority | Indicates the value of the 802.1p priority which is associated with the remote system connected to the port.                                                                                                                                                                                                                                  |
| PolicyDscp     | This object 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  | A value of true indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID, the Layer 2 priority, and the DSCP value fields are ignored. A value of false indicates that this network policy is defined.                                                                            |
| PolicyTagged   | A value of true indicates that the application is using a tagged VLAN. A value of false indicates that for the specific application, the device is using an untagged VLAN or does not support a port based VLAN operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance. |

---

## Neighbor Location

This section contains information about the following topics:

- [Viewing LLDP neighbor location properties](#) on page 312
- [Viewing coordinate-based location details](#) on page 313
- [Viewing civic address location details](#) on page 314

### Viewing LLDP neighbor location properties

With the Neighbor Location tab, you can view LLDP location properties for the remote system.

To view the Neighbor Location tab:

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Location** tab.

The following table outlines the parameters of the **Port MED Neighbor Location** tab.



**Table 192: Variable definitions**

| Variable        | Value                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark        | The TimeFilter for this entry.                                                                                                                                                                                  |
| LocalPortNum    | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index           | An 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 | The location subtype advertised by the remote device: <ul style="list-style-type: none"> <li>• unknown</li> <li>• coordinateBased</li> <li>• civicAddress</li> <li>• elin</li> </ul>                            |
| LocationInfo    | The location information advertised by the remote device. The parsing of this information is dependent on the location subtype.                                                                                 |

## Viewing coordinate-based location details

From the Neighbor Location tab, you can select coordinate-based locations and view details for the remote system.

To view coordinate-based location details:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Location** tab.
6. Select a location with the **LocationSubtype** listed as coordinateBased  
The Location Details button is activated.
7. Click the **Location Details** button.  
The Coordinate Based Location window displays the selected location details.
8. Click **Close**.

## Viewing civic address location details

From the Neighbor Location tab, you can select civic address locations and view details for the remote system.

To view civic address location details:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor Location** tab.
6. Select a location with the **LocationSubtype** listed as `civicAddress`  
The Location Details button is activated.
7. Click the **Location Details** button.  
The Civic Address Location window displays the selected location details.
8. Click **Close**.

---

## Viewing LLDP neighbor PoE properties

With the Neighbor PoE tab, you can view LLDP PoE properties for the remote system.

To view the Neighbor PoE tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor PoE** tab.

The following table outlines the parameters of the **Port MED Neighbor PoE** tab.

**Table 193: Variable definitions**

| Variable | Value                          |
|----------|--------------------------------|
| TimeMark | The TimeFilter for this entry. |

| Variable      | Value                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LocalPortNum  | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index         | An 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 | The type of PoE device.                                                                                                                                                                                         |

## Viewing LLDP neighbor PoE PSE properties

With the Neighbor PoE PSE tab, you can view LLDP PoE PSE properties for the remote system.

To view the Neighbor PoE PSE tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor PoE PSE** tab.

The following table outlines the parameters of the **Port MEDNeighbor PoE PSE** tab.

**Table 194: Variable definitions**

| Variable          | Value                                                                                                                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark          | The TimeFilter for this entry.                                                                                                                                                                                  |
| LocalPortNum      | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index             | An 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.                                                                                                                                           |

| Variable         | Value                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <ul style="list-style-type: none"> <li>• primary: indicates that the device advertises its power source as primary.</li> <li>• backup: indicates that the device advertises its power source as backup.</li> </ul>                                                                                                                                                                                                                 |
| PSEPowerPriority | <p>Specifies the priority advertised by the PSE connected remotely to the port:</p> <ul style="list-style-type: none"> <li>• critical: indicates that the device advertises its power priority as critical, see RFC 3621.</li> <li>• high: indicates that the device advertises its power priority as high, see RFC 3621.</li> <li>• low: indicates that the device advertises its power priority as low, see RFC 3621.</li> </ul> |

---

## Viewing LLDP neighbor PoE PD properties

With the Neighbor PoE PD tab, you can view LLDP PoE PD properties for the remote system.

To view the Neighbor PoE PD tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor PoE PD** tab.

The following table outlines the parameters of the **Port MED Neighbor PoE PD** tab.

**Table 195: Variable definitions**

| Variable     | Value                                                                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TimeMark     | The TimeFilter for this entry.                                                                                                                                                                                  |
| LocalPortNum | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index        | An 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                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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: <ul style="list-style-type: none"> <li>• fromPSE: indicates that the device advertises its power source as received from a PSE.</li> <li>• local: indicates that the device advertises its power source as local.</li> <li>• localAndPSE: indicates that the device advertises its power source as using both local and PSE power.</li> </ul>              |
| PDPowerPriority | Defines the priority advertised as being required by the PD connected remotely to the port: <ul style="list-style-type: none"> <li>• critical: indicates that the device advertises its power priority as critical, see RFC 3621.</li> <li>• high: indicates that the device advertises its power priority as high, see RFC 3621.</li> <li>• low: indicates that the device advertises its power priority as low, see RFC 3621.</li> </ul> |

## Viewing LLDP neighbor inventory properties

With the Neighbor Inventory tab, you can view LLDP Inventory properties for the remote system.

To view the Neighbor Inventory tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **802.1AB**.
4. From the 802.1AB tree, double-click **Port MED**.
5. Select the **Neighbor inventory** tab.

The following table outlines the parameters of the **Port MED Neighbor Inventory** tab.

**Table 196: Variable definitions**

| Variable | Value                          |
|----------|--------------------------------|
| TimeMark | The TimeFilter for this entry. |

| Variable     | Value                                                                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LocalPortNum | Identifies the local port on which the remote system information is received.                                                                                                                                   |
| Index        | An 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  | The vendor-specific hardware revision string as advertised by the remote device.                                                                                                                                |
| FirmwareRev  | The vendor-specific firmware revision string as advertised by the remote device.                                                                                                                                |
| SoftwareRev  | The vendor-specific software revision string as advertised by the remote device.                                                                                                                                |
| SerialNum    | The vendor-specific serial number as advertised by the remote device.                                                                                                                                           |
| MfgName      | The vendor-specific manufacturer name as advertised by the remote device.                                                                                                                                       |
| ModelName    | The vendor-specific model name as advertised by the remote device.                                                                                                                                              |
| AssetID      | The vendor-specific asset tracking identifier as advertised by the remote device.                                                                                                                               |

---

## LLDP MED policy management using Enterprises Device Manager

Use the information in this section to view, create, and edit LLDP MED policies for the switch.

---

### Navigation

- [Viewing LLDP MED policies](#) on page 319
- [Creating LLDP MED policies](#) on page 320
- [Editing LLDP MED policies](#) on page 321
- [Deleting LLDP MED policies](#) on page 323

## Viewing LLDP MED policies

Use this procedure to view LLDP MED policy properties for the local system.

### Procedure steps

1. Open one of the supported browsers.
2. Enter the IP address of the switch to open an EDM session.
3. From the navigation tree, double-click **Edit**.
4. In the Edit tree, double-click **Diagnostics**.
5. In the Diagnostic tree, double-click **802.1AB**.
6. In the 802.1AB tree, double-click **Port MED**.
7. In the work area, click the **Local Policy** tab.

Use the data in the following table to help you understand the LLDP MED local policy display.

**Table 197: Variable definitions**

| 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.                                                                                                                                                                                                                                                                                                                      |
| 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.                                                                                                                                                                                                                                  |
| 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

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 boxes.
10. To select a VLAN identifier for the selected port, click the **PolicyVlanID** elipsis.
11. Click **Ok** .
12. Double-click the **PolicyPriority** box.
13. Type a priority value.
14. Double-click the **PolicyDscp** box.
15. Type a DSCP value.
16. To use a tagged VLAN, click the **PolicyTagged** box.

OR

To use an untagged VLAN, clear the **PolicyTagged** box.

17. Click **Insert** .

Use the data in the following table to create a new LLDP MED policy for the local system.

**Table 198: Variable definitions**

| Field         | Description                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PortNum       | Specifies the port on which to configure LLDP MED policies.                                                                                                                                            |
| PolicyAppType | Specifies the policy application type. <ul style="list-style-type: none"> <li>• voice—selects the voice network policy</li> <li>• voiceSignaling—selects the voice signaling network policy</li> </ul> |



| Field          | Description                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                                                                                                                              |
| 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.                                                                                                                                                                                   |
| PolicyTagged   | Specifies the type of VLAN tagging to apply on the selected switch port or ports. <ul style="list-style-type: none"> <li>• when selected—uses a tagged VLAN</li> <li>• when cleared—uses an untagged VLAN or does not support port-based VLANs.</li> </ul> <p>If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.</p> |

---

## Editing LLDP MED policies

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. On the toolbar, click **Apply** .

Use the data in the following table to edit a previously configured LLDP MED policy for the local system.

**Table 199: Variable definitions**

| Field          | Description                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. <ul style="list-style-type: none"> <li>• voice— voice network policy</li> <li>• voiceSignaling— voice signaling network policy</li> </ul>                                                                                                                                                        |
| 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.                                                                                                                                                                                                                                              |
| 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.                                                                                                                                                                   |
| PolicyTagged   | Specifies the type of VLAN tagging to apply on the selected switch port or ports. <ul style="list-style-type: none"> <li>• true—uses a tagged VLAN</li> <li>• false—uses an untagged VLAN or does not support port-based VLANs.</li> </ul> <p>If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.</p> |

---

## Deleting LLDP MED policies

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. On the toolbar, click **Delete** .

---

## SNTP configuration using Enterprise Device Manager

The SNTP/Clock screen contains the parameters for configuring Simple Network Time Protocol (SNTP).

This section provides information about the following topics:

- [Displaying the Simple Network Time Protocol tab](#) on page 323
- [Setting the local time zone](#) on page 324
- [Configuring daylight savings time](#) on page 325
- [Displaying the Summer Time Recurring tab](#) on page 326

---

## Displaying the Simple Network Time Protocol tab

To open the Simple Network Time Protocol tab:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **SNTP/Clock**.
3. Select the **Simple Network Time Protocol** tab.
4. Enter the fields as indicated by the table.
5. Click **Refresh**.

The following table outlines the parameters of the **Simple Network Time Protocol** tab.

**Table 200: Variable definitions**

| Variable                           | Value                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PrimaryServerInet<br>AddressType   | The IP address type (IPv4 or IPv6) of the primary SNTP server.                                                                                                                                                                                                                                                                                                       |
| PrimaryServerInet<br>Address       | The IP address of the primary SNTP server.                                                                                                                                                                                                                                                                                                                           |
| SecondaryServerInet<br>AddressType | The IP address type (IPv4 or IPv6) of the secondary SNTP server.                                                                                                                                                                                                                                                                                                     |
| SecondaryServerInet<br>Address     | The IP address of the secondary SNTP server.                                                                                                                                                                                                                                                                                                                         |
| State                              | Controls whether the device uses the Simple Network Time Protocol to synchronize the device clock to the Coordinated Universal Time. If the value is disabled, the device does not synchronize its clock using SNTP.<br>If the value is unicast, the device synchronizes shortly after boot time when network access becomes available, and periodically thereafter. |
| SynchInterval                      | Controls the frequency, in hours, with which the device attempts to synchronize with the NTP servers.                                                                                                                                                                                                                                                                |
| ManualSynch Request                | Specifies that the device must immediately attempt to synchronize with the NTP servers.                                                                                                                                                                                                                                                                              |
| LastSynch Time                     | Specifies the UTC when the device last synchronized with an NTP server.                                                                                                                                                                                                                                                                                              |
| LastSyncSourceInet<br>AddressType  | Specifies the IP source address type (IPv4 or IPv6) of the NTP server with which this device last synchronized.                                                                                                                                                                                                                                                      |
| LastSyncSourceInet<br>Address      | Specifies the IP source address of the NTP server with which this device last synchronized.                                                                                                                                                                                                                                                                          |
| NextSynch Time                     | Specifies the UTC at which the next synchronization is scheduled.                                                                                                                                                                                                                                                                                                    |
| PrimaryServer<br>SynchFailures     | Specifies the number of times the switch failed to synchronize with the primary server address. However, synchronization with the secondary server address can still occur.                                                                                                                                                                                          |
| SecondaryServer<br>SynchFailures   | Specifies the number of times the switch failed to synchronize with the secondary server address.                                                                                                                                                                                                                                                                    |
| CurrentTime                        | Specifies the UTC for the switch.                                                                                                                                                                                                                                                                                                                                    |

---

## Setting the local time zone

To set the local time zone:

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **SNTP/Clock**.
3. Select the **Time Zone** tab.
4. Type the time zone offset in the **TimeZone** box.
5. Type a time zone acronym in the **TimeZoneAcronym** box.
6. Click **Apply**.

The following table outlines the parameters of the **Time Zone** tab.

**Table 201: Variable definitions**

| Variable        | Value                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| TimeZone        | Specifies the time zone of the switch, measured as an offset in 15-minute increments from Greenwich mean Time (GMT). |
| TimeZoneAcronym | Enter the acronym for your time zone: example, EST for Eastern Time Zone in North America.                           |

---

## Configuring daylight savings time

To set daylight saving start and end time:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **SNTP/Clock**.
3. Select the **Daylight Saving Time** tab.
4. Type the number of minutes to shift the clock in the **Offset** box.
5. Type the time zone acronym for the change in the **TimeZoneAcronym** box.
6. Select the **StartYear**, **StartMonth**, **StartDate**, **StartHour** and type the **StartMinutes** (if applicable) to define when to switch the clock to daylight saving time.
7. Select the **EndYear**, **EndMonth**, **EndDate**, **EndHour** and type the **EndMinutes** (if applicable) to define when to switch the clock back to normal time. If you want to keep the same daylight saving time changeover dates, you can set the **EndYear** to a year in the future.
8. Click **Enabled** to enable daylight savings time.
9. Click **Apply**.

The following table outlines the parameters of the **Daylight Saving Time** tab.

**Table 202: Variable definitions**

| Variable        | Value                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------|
| Offset          | Specifies the time in minutes by which you want to change the time when daylight savings begins and 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.                          |
| EndHour         | Specifies the hour of the particular day when to end the daylight savings time.                           |
| Enabled         | Enables or disables day light saving time.                                                                |

---

## Displaying the Summer Time Recurring tab

To set summer time recurring:

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **SNTP/Clock**.
3. Select the **Summer Time Recurring** tab.

The following table outlines the parameters of the **Summer Time Recurring** tab.

**Table 203: Variable definitions**

| Variable             | Value                                                                                                                                                                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RecurringStartMonth  | Specifies the month of each year you want recurring daylight savings time to start.                                                                                                                                                                               |
| ReucrringStartWeek   | Specifies the week of the month you want recurring daylight savings time to start.                                                                                                                                                                                |
| 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.                                                                                                                                                                                  |
| 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. |

---

## Power over Ethernet configuration with Enterprise Device Manager

You can view and configure Power over Ethernet (PoE) for a unit or a port with Enterprise Device Manager.

---

## Navigation

- [Viewing global PoE properties for a unit](#) on page 328
- [Viewing PoE properties for a port](#) on page 329

---

## Viewing global PoE properties for a unit

To view the Globals - PoE Units tab:

### Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. From the Power Management tree, double-click **PoE**.
3. Select the **Globals - PoE Units** tab.

The following table outlines the parameters of the **Globals - PoE Units** tab.

**Table 204: Variable definitions**

| Variable                  | Value                                                                                                                                                                                                                  |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit                      | Specifies the unit number in the stack.                                                                                                                                                                                |
| Power(watts)              | Specifies the power in Watts.                                                                                                                                                                                          |
| OperStatus                | Specifies whether PoE is enabled                                                                                                                                                                                       |
| ConsumptionPower(watts)   | Specifies the power consumption in Watts.                                                                                                                                                                              |
| UsageThreshold%           | Specifies the usage threshold expressed as a percentage for comparing the measured power and initiating an alarm if the threshold is exceeded.                                                                         |
| NotificationControlEnable | Controls, on a per-group basis, whether or not notifications from the agent are enabled. The value true(1) means that notifications are enabled; the value false(2) means that they are not.                           |
| PoweredDeviceDetectType   | Specifies the mechanism used to detect powered ethernet devices attached to a powered ethernet port. This object should only be instantiated for values of ifIndex that represent ports that support powered ethernet. |

For more information, see [Displaying the PoE tab for a single unit](#) on page 219.



## Viewing PoE properties for a port

To view the PoE Ports tab:

### Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. From the Power Management tree, double-click **PoE**.
3. Select the **PoE Ports** tab.

The following table outlines the parameters of the **PoE Ports** tab.

**Table 205: Variable definitions**

| Variable             | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit                 | Indicates the switch position in a stack.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Port                 | Indicates the switch port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| AdminEnable          | Use this function to enable or disable Power over Ethernet on this port. PoE is enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| PowerPairs           | This is a read-only field that displays the status of the RJ-45 pin pairs that the switch uses to send power to the ports on the switch.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DetectionStatus      | <p>Displays the operational status of the power-device detecting mode on the specified port as follows:</p> <ul style="list-style-type: none"> <li>• disabled, detecting function disabled</li> <li>• searching, detecting function is enabled and the system is searching for a valid powered device and the port is delivering power</li> <li>• fault, power-specific fault detected on port</li> <li>• test, detecting device in test mode</li> <li>• otherFault</li> </ul> <p><b>!</b> <b>Important:</b><br/>Avaya recommends against using the test operational status.</p> |
| PowerClassifications | You can use classifications 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        | You can set the power priority for the specified port to:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Variable          | Value                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------|
|                   | <ul style="list-style-type: none"> <li>• critical</li> <li>• high</li> <li>• low</li> </ul> |
| 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.                                                     |

For more information, see [Viewing the PoE power settings](#) on page 234.

---

## IPv6 configuration using Enterprise Device Manager

To open the IPv6 dialog box:

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. From the IPv6 tree, double-click **IPv6**.

This section contains information about the following topics:

- [Configuring IPv6 global properties](#) on page 330
- [Displaying the ICMP Stats tab](#) on page 331
- [Displaying the ICMP Msg Stats tab](#) on page 332

---

## Configuring IPv6 global properties

To configure IPv6 global properties:

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. From the IPv6 tree, double-click **IPv6**.
3. Select the **Globals** tab.
4. Enter the global properties in the boxes.
5. Click **Apply** to save the changes.
6. Click **Refresh** to display updated information.

The following table outlines the parameters of the **Globals** tab.

**Table 206: Variable definitions**

| Variable             | Value                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| AdminEnabled         | Check this box to enable the administration function.                                                                                              |
| OperEnabled          | True or false                                                                                                                                      |
| Forwarding           | notForwarding or Forwarding                                                                                                                        |
| DefaultHopLimit      | Default number of hops: 30                                                                                                                         |
| IcmpNetUnreach       | Enables or disables the ICMP net unreachable feature.                                                                                              |
| IcmpRedirectMsg      | True or false                                                                                                                                      |
| IcmpErrorInterval    | Time to wait before sending an ICMP error message. A value of 0 means the system does not send an ICMP error message.<br>Value: 0 to 2147483647 ms |
| IcmpErrorQuota       | Default value: 1                                                                                                                                   |
| MulticastAdminStatus | True or false                                                                                                                                      |

## Displaying the ICMP Stats tab

To display the IPv6 interface ICMP statistics:

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. From the IPv6 tree, double-click **IPv6**.
3. Select the **ICMP Stats** tab.
4. Click **Clear Counters** to reset the statistics.
5. Set the Poll interval.

The following table outlines the parameters for the **ICMP Stats** window.

**Table 207: Variable definitions**

| Variable      | Value                                    |
|---------------|------------------------------------------|
| InMsgs        | Number of ICMP messages received.        |
| InErrors      | Number of ICMP error messages received.  |
| OutMsgs       | Number of ICMP messages sent.            |
| OutErrors     | Number of ICMP error messages sent.      |
| Poll Interval | Sets polling interval. Value: 2 to 60 s. |

---

## Displaying the ICMP Msg Stats tab

To display the IPv6 interface ICMP message statistics:

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. From the IPv6 tree, double-click **IPv6**.
3. Select the **ICMP Msg Stats** tab.
4. Click **Refresh** to update the ICMP message statistics.

The following table outlines the parameters for the **ICMP Msg Stats** window.

**Table 208: Variable definitions**

| Variable | Value                            |
|----------|----------------------------------|
| Type     | Type of packet received or sent. |
| InPkts   | Number of packets received.      |
| OutPkts  | Number of packets sent.          |

---

## Viewing SFP GBIC ports

The details of an SFP GBIC port are only available if the port is active.

To view the SFP GBIC ports:

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**.

# Chapter 8: Configuration reference

---

## Factory default configuration

When a newly installed switch is initially accessed or a switch is reset to factory defaults, the switch is in a factory default configuration. This factory default configuration is the base configuration from which the switch configuration is built.

[Table 209: Factory default configuration settings](#) on page 333 outlines the factory default configuration settings present in a switch in a factory default state.

**Table 209: 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                                 |
| Find an Address             | 00-00-00-00-00-00 (no MAC address assigned) |

| Setting                               | Factory Default Configuration Value       |
|---------------------------------------|-------------------------------------------|
| Select VLAN ID [1]                    |                                           |
| 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                                      |
| Current Learning Mode                 | Not Learning                              |
| Trunk                                 | blank field                               |
| Security                              | Disabled                                  |
| Port List                             | blank field                               |
| Find an Address                       | blank field                               |
| MAC Address                           | 00-00 00-00 -00-00                        |
| Allowed Source                        | - (blank field)                           |
| Display/Create MAC Address            | 00-00-00-00-00-00                         |
| Create VLAN                           | 1                                         |
| Delete VLAN                           | blank field                               |
| VLAN Name                             | VLAN #                                    |
| Management VLAN                       | Yes (VLAN #1)                             |
| VLAN Type                             | Port-based                                |
| Protocol ID (PID)                     | None                                      |
| User-Defined PID                      | 0x0000                                    |
| VLAN State                            | Active (VLAN # 1)                         |
| Port Membership                       | All ports assigned as members of VLAN 1   |
| Unit                                  | 1                                         |
| Port                                  | 1                                         |
| Filter Untagged Frames                | No                                        |

| Setting                    | Factory Default Configuration Value         |
|----------------------------|---------------------------------------------|
| Filter Unregistered Frames | Yes                                         |
| Port Name                  | Unit 1, Port 1                              |
| PVID                       | 1                                           |
| Port Priority              | 0                                           |
| Tagging                    | Untag All                                   |
| AutoPVID                   | Enabled                                     |
| Unit                       | 1                                           |
| Port                       | 1                                           |
| PVID                       | 1 (read only)                               |
| Port Name                  | Unit 1, Port 1 (read only)                  |
| Unit                       | 1                                           |
| Status                     | Enabled (for all ports)                     |
| Linktrap                   | On                                          |
| Autonegotiation            | Enabled (for all ports)                     |
| Speed/Duplex               | (Refer to Autonegotiation)                  |
| Trunk                      | 1 to 32 (depending on configuration status) |
| Trunk Members (Unit/Port)  | Blank field                                 |
| STP Learning               | Normal                                      |
| Trunk Mode                 | Basic                                       |
| Trunk Status               | Disabled                                    |
| Trunk Name                 | Trunk #1 to Trunk #32                       |
| Traffic Type               | Rx and Tx                                   |
| Port                       | 1                                           |
| Monitoring Mode            | Disabled                                    |
| Monitor/Unit Port          | Zero-length string                          |
| Unit/Port X                | Zero-length string                          |
| Unit/Port Y                | Zero-length string                          |
| Address A                  | 00-00-00-00-00-00 (no MAC address assigned) |
| Address B                  | 00-00-00-00-00-00 (no MAC address assigned) |
| Rate Limit Packet Type     | Both                                        |
| Limit                      | None                                        |

| Setting                            | Factory Default Configuration Value                                                        |
|------------------------------------|--------------------------------------------------------------------------------------------|
| VLAN                               | 1                                                                                          |
| Snooping                           | Disabled                                                                                   |
| Proxy                              | Disabled                                                                                   |
| Robust Value                       | 2                                                                                          |
| Query Time                         | 125 seconds                                                                                |
| Set Router Ports                   | Version 1                                                                                  |
| Static Router Ports                | - (for all ports)                                                                          |
| Multicast Group Membership screen  |                                                                                            |
| Unit                               | 1                                                                                          |
| Port                               | 1                                                                                          |
| Console Port Speed                 | 9600 Baud                                                                                  |
| Console Switch Password type       | None                                                                                       |
| Console Stack Password type        | None                                                                                       |
| Telnet Stack Password type         | None                                                                                       |
| Telnet Switch Password type        | None                                                                                       |
| Console Read-Only Switch Password  | Passwords are user for non-SSH software images and userpasswd for SSH software images.     |
| Console Read-Write Switch Password | Passwords are secure for non-SSH software images and securepasswd for SSH software images. |
| Console Read-Only Stack Password   | Passwords are user for non-SSH software images and userpasswd for SSH software images.     |
| Console Read-Write Stack Password  | Passwords are secure for non-SSH software images and securepasswd for SSH software images. |
| Radius password/server             | secret                                                                                     |
| New Unit Number                    | Current stack order                                                                        |
| Renumber units with new setting?   | No                                                                                         |
| Group                              | 1                                                                                          |
| Bridge Priority                    | 8000                                                                                       |
| Bridge Hello Time                  | 2 seconds                                                                                  |
| Bridge Maximum Age Time            | 20 seconds                                                                                 |
| Bridge Forward Delay               | 15 seconds                                                                                 |



| Setting                                                                             | Factory Default Configuration Value                                                                                                                                  |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add VLAN Membership                                                                 | 1                                                                                                                                                                    |
| Tagged BPDU on tagged port                                                          | <ul style="list-style-type: none"> <li>• STP Group 1--No</li> <li>• Other STP Groups--Yes</li> </ul>                                                                 |
| STP Group State                                                                     | <ul style="list-style-type: none"> <li>• STP Group 1--Active</li> <li>• Other STP Groups--InActive</li> </ul>                                                        |
| VID used for tagged BPDU                                                            | 4001-4008 for STGs 1-8, respectively                                                                                                                                 |
| STP Group                                                                           | 1                                                                                                                                                                    |
| Participation                                                                       | Normal Learning                                                                                                                                                      |
| Priority                                                                            | 128                                                                                                                                                                  |
| Path Cost                                                                           | 1                                                                                                                                                                    |
| STP Group                                                                           | 1                                                                                                                                                                    |
| STP Group                                                                           | 1                                                                                                                                                                    |
| TELNET Access/SNMP                                                                  | By default, SNMP access is disabled in the SSH image and enabled in the non-SSH image. Telnet is enabled by default in both SSH and non-SSH images.<br>Use list: Yes |
| Login Timeout                                                                       | 1 minute                                                                                                                                                             |
| Login Retries                                                                       | 3                                                                                                                                                                    |
| Inactivity Timeout                                                                  | 15 minutes                                                                                                                                                           |
| Event Logging                                                                       | All                                                                                                                                                                  |
| Allowed Source IP Address (50 user-configurable fields)                             | First field: 0.0.0.0 (no IP address assigned)                                                                                                                        |
|                                                                                     | Remaining 49 fields: 255.255.255.255 (any address is allowed)                                                                                                        |
| Allowed Source Mask (50 user-configurable fields)                                   | First field: 0.0.0.0 (no IP address assigned)                                                                                                                        |
|                                                                                     | Remaining 49 fields: 255.255.255.255 (any address is allowed)                                                                                                        |
| Allowed Source IPv6 Address and Allowed Prefix Length (50 user-configurable fields) | First field: ::/0 (no IPv6 address assigned)                                                                                                                         |
|                                                                                     | Remaining 49 fields: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 (any IPv6 address is allowed)                                                                       |
| Image Filename                                                                      | Zero-length string                                                                                                                                                   |
| Diagnostics image filename                                                          | Zero-length string                                                                                                                                                   |

| Setting                                  | Factory Default Configuration Value |
|------------------------------------------|-------------------------------------|
| TFTP Server IP Address                   | 0.0.0.0 (no IP address assigned)    |
| Start TFTP Load of New Image             | No                                  |
| Configuration Image Filename             | Zero-length string                  |
| Copy Configuration Image to Server       | No                                  |
| Retrieve Configuration Image from Server | No                                  |
| ASCII Configuration Filename             | Zero-length string                  |
| Retrieve Configuration file from Server  | No                                  |
| Auto Configuration on Reset              | Disabled                            |
| EAPOL Security Configuration             | Disabled                            |
| High Speed Flow Control Configuration    |                                     |
| VLAN Configuration Control               | Strict                              |
| Agent Auto Unit Replacement              | Enabled                             |

## Index

---

### A

|                                   |                                         |
|-----------------------------------|-----------------------------------------|
| AAUR .....                        | <a href="#">199</a>                     |
| access .....                      | <a href="#">132</a>                     |
| address field .....               | <a href="#">83</a>                      |
| address source field .....        | <a href="#">83</a>                      |
| AdminState field .....            | <a href="#">226</a>                     |
| Agent Auto Unit Replacement ..... | <a href="#">199</a>                     |
| AUR .....                         | <a href="#">196</a>                     |
| configuring with ACLI .....       | <a href="#">196</a>                     |
| auto-MDI X .....                  | <a href="#">48</a>                      |
| autonegotiation .....             | <a href="#">48</a> , <a href="#">86</a> |
| description .....                 | <a href="#">48</a>                      |
| autopolarity .....                | <a href="#">48</a>                      |
| autosense description .....       | <a href="#">48</a>                      |
| Autotopology .....                | <a href="#">90</a>                      |
| configuring with ACLI .....       | <a href="#">90</a>                      |
| autotopology command .....        | <a href="#">91</a>                      |
| available power .....             | <a href="#">219</a>                     |

---

### B

|                           |                                           |
|---------------------------|-------------------------------------------|
| banner command .....      | <a href="#">195</a>                       |
| BaseNumPorts field .....  | <a href="#">226</a>                       |
| boot command .....        | <a href="#">134</a>                       |
| Bootp .....               | <a href="#">36</a>                        |
| BootP .....               | <a href="#">83</a> , <a href="#">135</a>  |
| modes .....               | <a href="#">135</a>                       |
| bootp field .....         | <a href="#">83</a>                        |
| Bridge parameter .....    | <a href="#">253</a> , <a href="#">255</a> |
| Base tab .....            | <a href="#">253</a>                       |
| BridgeAddress field ..... | <a href="#">253</a>                       |
| NumPorts field .....      | <a href="#">253</a>                       |
| Type .....                | <a href="#">253</a>                       |
| Forwarding tab .....      | <a href="#">255</a>                       |
| Address field .....       | <a href="#">255</a>                       |
| Port field .....          | <a href="#">255</a>                       |
| Status field .....        | <a href="#">255</a>                       |
| broadcast traffic .....   | <a href="#">94</a>                        |

---

### C

|                              |                                          |
|------------------------------|------------------------------------------|
| CANA .....                   | <a href="#">49</a> , <a href="#">104</a> |
| configuring with NNCLI ..... | <a href="#">104</a>                      |
| Clock .....                  | <a href="#">147</a>                      |
| configuring with ACLI .....  | <a href="#">147</a>                      |

|                                             |                     |
|---------------------------------------------|---------------------|
| configuration files .....                   | <a href="#">124</a> |
| in ACLI .....                               | <a href="#">124</a> |
| connecting external power source .....      | <a href="#">60</a>  |
| ConsumptionPower field .....                | <a href="#">219</a> |
| Custom Autonegotiation Advertisements ..... | <a href="#">49</a>  |

---

### D

|                                                  |                     |
|--------------------------------------------------|---------------------|
| DC power source .....                            | <a href="#">60</a>  |
| connection .....                                 | <a href="#">60</a>  |
| default autotopology command .....               | <a href="#">91</a>  |
| default duplex command .....                     | <a href="#">88</a>  |
| default flowcontrol command .....                | <a href="#">93</a>  |
| default ip address unit command .....            | <a href="#">85</a>  |
| default ipbootp server command .....             | <a href="#">136</a> |
| default management interface .....               | <a href="#">131</a> |
| setting .....                                    | <a href="#">131</a> |
| default rate-limit command .....                 | <a href="#">96</a>  |
| default speed command .....                      | <a href="#">87</a>  |
| default telnet-access command .....              | <a href="#">134</a> |
| default-gateway field .....                      | <a href="#">83</a>  |
| Descr field .....                                | <a href="#">226</a> |
| DHCP .....                                       | <a href="#">46</a>  |
| dhcp client lease field .....                    | <a href="#">83</a>  |
| DNS .....                                        | <a href="#">107</a> |
| configuring with ACLI .....                      | <a href="#">107</a> |
| duplex command .....                             | <a href="#">88</a>  |
| duplex mode .....                                | <a href="#">86</a>  |
| Dynamic Host Configuration Protocol (DHCP) ..... | <a href="#">46</a>  |

---

### E

|                             |                    |
|-----------------------------|--------------------|
| external power source ..... | <a href="#">60</a> |
| connecting .....            | <a href="#">60</a> |

---

### F

|                                     |                     |
|-------------------------------------|---------------------|
| factory default configuration ..... | <a href="#">333</a> |
| feature license file .....          | <a href="#">203</a> |
| configuring with NNCLI .....        | <a href="#">203</a> |
| flow control .....                  | <a href="#">92</a>  |
| flowcontrol command .....           | <a href="#">92</a>  |
| Forwarding tab .....                | <a href="#">255</a> |

|                                                 |                              |
|-------------------------------------------------|------------------------------|
| <b>G</b>                                        |                              |
| gateway .....                                   | <a href="#">79</a>           |
| GBIC information .....                          | <a href="#">196</a>          |
| displaying .....                                | <a href="#">196</a>          |
| Gigabit Ethernet .....                          | <a href="#">92</a>           |
| <hr/>                                           |                              |
| <b>H</b>                                        |                              |
| hardware information .....                      | <a href="#">196</a>          |
| displaying .....                                | <a href="#">196</a>          |
| <hr/>                                           |                              |
| <b>I</b>                                        |                              |
| IEEE 802.3u standard .....                      | <a href="#">48</a>           |
| interfaces .....                                | <a href="#">85</a>           |
| displaying .....                                | <a href="#">85</a>           |
| IP address .....                                | <a href="#">79–81, 84</a>    |
| for each unit .....                             | <a href="#">84</a>           |
| ip address command .....                        | <a href="#">80</a>           |
| ip address unit command .....                   | <a href="#">84</a>           |
| IP blocking .....                               | <a href="#">78</a>           |
| configuring with ACLI .....                     | <a href="#">78</a>           |
| ip bootp server command .....                   | <a href="#">135</a>          |
| ip default-gateway command .....                | <a href="#">82</a>           |
| IpAddress field .....                           | <a href="#">226</a>          |
| <hr/>                                           |                              |
| <b>L</b>                                        |                              |
| LLDP .....                                      | <a href="#">164</a>          |
| Configuring with ACLI .....                     | <a href="#">164</a>          |
| Location field .....                            | <a href="#">226</a>          |
| LstChng field .....                             | <a href="#">226</a>          |
| <hr/>                                           |                              |
| <b>M</b>                                        |                              |
| MDAs .....                                      | <a href="#">92</a>           |
| multicast traffic .....                         | <a href="#">94</a>           |
| <hr/>                                           |                              |
| <b>N</b>                                        |                              |
| netmask .....                                   | <a href="#">80, 84</a>       |
| no autotopology command .....                   | <a href="#">91</a>           |
| no banner command .....                         | <a href="#">195</a>          |
| no flowcontrol command .....                    | <a href="#">93</a>           |
| no ip address command .....                     | <a href="#">81</a>           |
| no ip address unit command .....                | <a href="#">84</a>           |
| no ip bootp server command .....                | <a href="#">136</a>          |
| no ip default-gateway .....                     | <a href="#">82</a>           |
| no rate-limit command .....                     | <a href="#">95</a>           |
| no telnet-access command .....                  | <a href="#">133</a>          |
| NotificationControlEnable field .....           | <a href="#">219</a>          |
| NVRAM .....                                     | <a href="#">74</a>           |
| <hr/>                                           |                              |
| <b>O</b>                                        |                              |
| OperState field .....                           | <a href="#">226, 243</a>     |
| OperStatus field .....                          | <a href="#">219</a>          |
| <hr/>                                           |                              |
| <b>P</b>                                        |                              |
| passwords .....                                 | <a href="#">204</a>          |
| setting with NNCLI .....                        | <a href="#">204</a>          |
| ping command .....                              | <a href="#">106</a>          |
| PoE .....                                       | <a href="#">60, 190, 219</a> |
| available power .....                           | <a href="#">219</a>          |
| configuring with ACLI .....                     | <a href="#">190</a>          |
| power being used .....                          | <a href="#">219</a>          |
| error codes .....                               | <a href="#">60</a>           |
| status codes .....                              | <a href="#">60</a>           |
| traps .....                                     | <a href="#">219</a>          |
| ports .....                                     | <a href="#">86</a>           |
| power being used .....                          | <a href="#">219</a>          |
| Power field .....                               | <a href="#">219</a>          |
| power usage traps .....                         | <a href="#">219</a>          |
| PowerDetectionMethod fieldtroubleshooting ..... | <a href="#">219</a>          |
| power detection method .....                    | <a href="#">219</a>          |
| PowerPairs field .....                          | <a href="#">219</a>          |
| <hr/>                                           |                              |
| <b>Q</b>                                        |                              |
| quick configuration .....                       | <a href="#">76</a>           |
| <hr/>                                           |                              |
| <b>R</b>                                        |                              |
| RADIUS authentication .....                     | <a href="#">206</a>          |
| configuring with ACLI .....                     | <a href="#">206</a>          |
| rate-limit command .....                        | <a href="#">94</a>           |
| rate-limiting .....                             | <a href="#">94</a>           |
| Real Time Clock .....                           | <a href="#">102</a>          |
| configuring with NNCLI .....                    | <a href="#">102</a>          |
| reload command .....                            | <a href="#">137</a>          |
| RelPos field .....                              | <a href="#">226</a>          |
| requirements .....                              | <a href="#">131</a>          |
| remote access .....                             | <a href="#">131</a>          |
| <hr/>                                           |                              |
| <b>S</b>                                        |                              |
| security .....                                  | <a href="#">132</a>          |
| SerNum field .....                              | <a href="#">226</a>          |

|                                           |                         |                                                 |                                 |
|-------------------------------------------|-------------------------|-------------------------------------------------|---------------------------------|
| setting TFTP parameters with NNCLI .....  | <a href="#">23</a>      | IEEE 802.1 organizationally-specific .....      | <a href="#">68</a>              |
| show banner command .....                 | <a href="#">194</a>     | IEEE 802.3 organizationally-specific .....      | <a href="#">68</a>              |
| show interfaces command .....             | <a href="#">86</a>      | Management .....                                | <a href="#">67</a>              |
| show ip command .....                     | <a href="#">83</a>      | Organizationally-specific for MED devices ..... | <a href="#">68</a>              |
| show rate-limit command .....             | <a href="#">94</a>      | TotalNumPorts .....                             | <a href="#">226</a>             |
| shutdown command .....                    | <a href="#">136</a>     | traffic .....                                   | <a href="#">92, 94</a>          |
| Simple Network Time Protocol .....        | <a href="#">96</a>      | Gigabit Ethernet .....                          | <a href="#">92</a>              |
| Simple Network Time Protocol (SNTP) ..... | <a href="#">47</a>      | rate-limiting .....                             | <a href="#">94</a>              |
| SNTP .....                                | <a href="#">47, 96</a>  | Transparent tab .....                           | <a href="#">254</a>             |
| configuring with NNCLI .....              | <a href="#">96</a>      | traps .....                                     | <a href="#">219</a>             |
| software .....                            | <a href="#">23, 122</a> | power .....                                     | <a href="#">219</a>             |
| updating .....                            | <a href="#">23</a>      | troubleshooting .....                           | <a href="#">60, 81, 84, 219</a> |
| updating with ACLI .....                  | <a href="#">122</a>     | DC power source .....                           | <a href="#">60</a>              |
| speed .....                               | <a href="#">86</a>      | power pairs .....                               | <a href="#">219</a>             |
| speed command .....                       | <a href="#">86</a>      | access .....                                    | <a href="#">81, 84</a>          |
| subnet mask .....                         | <a href="#">80, 84</a>  | external power source .....                     | <a href="#">60</a>              |
| switch configuration .....                | <a href="#">74</a>      | PoE .....                                       | <a href="#">219</a>             |
|                                           |                         | Type field .....                                | <a href="#">226</a>             |

## T

|                             |                          |
|-----------------------------|--------------------------|
| TDR .....                   | <a href="#">89</a>       |
| configuring with ACLI ..... | <a href="#">89</a>       |
| Telnet .....                | <a href="#">131, 132</a> |
| telnet command .....        | <a href="#">107</a>      |
| telnet-access command ..... | <a href="#">132</a>      |
| terminal setup .....        | <a href="#">130</a>      |
| testing cables .....        | <a href="#">89</a>       |
| TLVs .....                  | <a href="#">67, 68</a>   |

## U

|                               |                     |
|-------------------------------|---------------------|
| updating software .....       | <a href="#">23</a>  |
| UsageThreshold field .....    | <a href="#">219</a> |
| user access limitations ..... | <a href="#">204</a> |
| setting with NNCLI .....      | <a href="#">204</a> |

## V

|                 |                     |
|-----------------|---------------------|
| Ver field ..... | <a href="#">226</a> |
| VlanIds .....   | <a href="#">255</a> |

