



# **Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series**

Release 7.8.1  
9036741-00 Rev. AA  
July 2020

© 2017-2020, Extreme Networks, Inc.  
All Rights Reserved.

### **Legal Notice**

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

### **Trademarks**

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see:  
[www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks)

### **Open Source Declarations**

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>

# Contents

<b>Chapter 1: About this Document</b> .....	10
Purpose.....	10
Conventions.....	10
Text Conventions.....	10
Documentation and Training.....	12
Getting Help.....	13
Providing Feedback.....	14
<b>Chapter 2: New in this document</b> .....	15
<b>Chapter 3: System Configuration</b> .....	16
System Configuration Fundamentals.....	16
Feature Licensing.....	16
Hardware features.....	17
Stacking Capabilities.....	21
Auto Unit Replacement.....	22
Diagnostic Auto Unit Replacement.....	29
Stack Forced Mode.....	30
IPv6 Management.....	31
Jumbo frames.....	39
Flash memory storage.....	39
Policy-enabled networking.....	40
Port Mirroring.....	41
Rate Limiting.....	41
Auto-MDI/X.....	42
Auto-polarity.....	42
Time Domain Reflectometer.....	43
Autosensing and Autonegotiation.....	43
Oversubscription and 2.5 Gbps support.....	44
ASCII Configuration File.....	44
Backup configuration file.....	49
Booting with an ASCII Configuration File from the Local System.....	50
Displaying unit uptime.....	50
Port naming.....	50
Port error summary.....	51
IP address for each unit in a stack.....	51
BootP automatic IP Configuration and MAC Address.....	51
DHCP client.....	52
Web Quick Start.....	52
Simple Network Time Protocol.....	52
Link-state tracking.....	53

Ping enhancement.....	56
New Unit Quick Configuration.....	57
Updating Switch Software.....	57
Asset ID string configuration.....	58
Energy Saver.....	58
Secure Shell File Transfer Protocol (SFTP over SSH).....	60
SFTP Server .....	60
EDM inactivity time-out.....	61
Custom logon banner.....	61
Run Scripts.....	61
Factory default configuration.....	64
Configuring System using CLI.....	68
Configuring Feature licenses using CLI.....	68
Setting User Access Limitations.....	71
Configuring Run Script.....	74
Change Switch Software.....	78
Toggle the Dual Agent next Boot Image.....	79
Setting TFTP Parameters.....	80
Configuring SFTP using CLI.....	82
Configuring files in CLI.....	83
Configuring Terminal Settings.....	116
Set Telnet Access.....	117
Set Boot Parameters.....	118
View the Agent and Image Software Load Status.....	120
Configuring BootP.....	121
Customizing the CLI Logon Banner.....	123
Display Help Text on CLI Commands.....	125
Configuring Auto Unit Replacement.....	125
Managing and Configuring Agent Auto Unit Replacement.....	127
Configure Stack Forced Mode.....	128
Display Stack Cable Information.....	129
Display Complete GBIC Information.....	129
Display Hardware Information.....	130
Shut Down a Switch.....	131
Reload Remote Devices.....	132
Restore the Factory Default Configuration.....	133
Viewing IPv4 Socket Information.....	133
Configuring IPv6.....	135
Configuring Link-state.....	150
Administering General Switch using the CLI.....	153
Configuring LLDP using CLI.....	193
Configuring Asset ID String.....	226
Configuring Energy Saver.....	228

Enable or Disable UTC Timestamp in CLI show command Outputs.....	235
Enable the Web Server for EDM.....	235
Configure the EDM Inactivity Time Out using CLI.....	235
Configuring Jumbo Frames.....	236
Configuring System using the EDM.....	238
Configure Quick Start using EDM.....	238
Configure Out-Of-Band Management using EDM.....	239
Configure Remote Access using EDM.....	240
Configure the IPv4 Remote Access List using EDM.....	241
Configure the IPv6 Remote Access List using EDM.....	242
Customizing the EDM Logon Banner.....	243
Running Script Configuration using EDM.....	244
View Switch Unit Information using EDM.....	249
Unit statistics management.....	250
Configuring System Parameters using the EDM.....	251
Configuring Asset ID using EDM.....	254
Configuring AUR using EDM.....	255
Configuring a Switch Stack Base Unit using EDM.....	256
Renumbering Stack Switch Units using EDM.....	257
Managing Switch Interface Port Configurations using EDM.....	257
Configuring Rate Limiting using EDM.....	264
View USB Files.....	265
Manage Switch Software using EDM.....	265
ASCII Configuration File Management using EDM.....	268
Manage the License File using EDM.....	271
Save the Current Configuration using EDM.....	273
View Flash Information using EDM.....	274
Configure IPv6 Global Properties using EDM.....	275
IPv6 Interface Management using EDM.....	277
Graph IPv6 Interface Statistics using EDM.....	279
Graph IPv6 Interface ICMP Statistics.....	281
Configure an IPv6 Address using EDM.....	282
View the IPv6 Routing Table.....	283
Configure an IPv6 Discovery Prefix.....	285
Configure IPv6 Router Advertisement.....	287
IPv6 Neighbor Cache Management using EDM.....	289
Graph IPv6 Interface ICMP Statistics using EDM.....	291
View ICMP Message Statistics using EDM.....	292
Display IPv6 TCP Global Properties using EDM.....	292
Display IPv6 TCP Connections using EDM.....	293
Display IPv6 TCP Listeners using EDM.....	293
Display IPv6 UDP Endpoints using EDM.....	294
View SFP GBIC Ports using EDM.....	295

View Basic System Bridge Information using EDM.....	295
Initiate a Cable Diagnostic Test using EDM.....	295
View Transparent Bridge Information using EDM.....	298
View Forwarding Bridge Information using EDM.....	299
Graph Port Bridge Statistics using EDM.....	300
Configure SNTP using EDM.....	300
Configure the Local Time Zone using EDM.....	302
Configure Daylight Savings Time using EDM.....	302
Configure Recurring Daylight Saving Time using EDM.....	304
Link-State Configuration using EDM.....	306
View Network Topology Information using EDM.....	307
View the Topology Table using EDM.....	308
Enable or Disable TLV Transmit Flags using EDM.....	309
Configure the Switch Call Server IP Address TLV using EDM.....	311
Configure the Switch File Server IP Address TLV using EDM.....	312
View IP Phone Power Level TLV Information using EDM.....	313
View Remote Call Server IP Address TLV Information using EDM.....	314
View Remote File Server IP Address TLV Information using EDM.....	314
View Remote 802.1Q Framing TLV information using EDM.....	315
View Remote IP TLV Information using EDM.....	316
Configuring Global Energy Saver using EDM.....	316
Configuring Energy Saver schedule using EDM.....	319
Configuring Port-based Energy Saver using EDM.....	321
Viewing Energy Saver Information using EDM.....	322
<b>Chapter 4: Network Time Protocol</b> .....	<b>324</b>
NTP Fundamentals.....	324
NTP terms.....	325
NTP system implementation model.....	325
Time distribution within a subnet.....	326
Synchronization.....	327
NTP modes of operation.....	327
NTP Authentication.....	328
Configuring NTP using the CLI.....	329
Prerequisites to NTP Configuration.....	329
NTP configuration procedures.....	329
Configuring System Clock.....	330
Enable NTP Globally.....	332
Create Authentication Keys.....	333
Configure an NTP Server.....	334
Modify Options for an NTP Server.....	334
Display NTP Settings.....	335
Configuring NTP using the EDM.....	336
Configuring NTP using the EDM.....	337

Enable NTP Globally using EDM.....	337
Add or Remove an NTP Server using EDM.....	338
Configure Authentication Keys using EDM.....	339
<b>Chapter 5: Power over Ethernet.....</b>	<b>341</b>
Power over Ethernet Fundamentals.....	341
PoE Overview.....	341
PoE high inrush mode.....	343
PoE Power Priority and Limit for IP Phones.....	343
LLDP support for PoE+.....	343
Port power priority.....	344
Configuring Power over Ethernet using the CLI.....	345
Enable Port Power.....	345
Disable Port Power.....	346
Set Port Power Priority.....	346
Set Power Limit for Channels.....	347
Configure PoE Power Up Mode.....	347
Display PoE Main Configuration.....	348
Set a Power Usage Threshold.....	348
Set the Method to Detect Power Devices.....	349
Display PoE Port Configuration.....	350
Display PoE Power Measurement.....	351
Download PoE Firmware from SFTP.....	351
Configure PoE Priority for IP Phone.....	351
Disable PoE Priority and Power Limit.....	352
Configuring Power over Ethernet using EDM.....	353
View PoE Ports using EDM.....	353
Managing PoE for a Switch Unit using the EDM.....	353
Managing Power over Ethernet (PoE) using EDM.....	354
Configuring PoE for Switch Ports using EDM.....	356
Configuring the PoE Conservation Level Request TLV using the EDM.....	362
View PoE Conservation Level Support TLV Information using EDM.....	364
<b>Chapter 6: Link Layer Discovery Protocol (802.1ab).....</b>	<b>365</b>
Link Layer Discovery Protocol Fundamentals.....	365
Link Layer Discovery Protocol (IEEE 802.1AB) Overview.....	365
Connectivity and Management Information.....	366
Configuring LLDP using CLI.....	373
Set LLDP Transmission Parameters.....	373
Set LLDP Port Parameters.....	374
Set LLDP Media Endpoint Devices (MED).....	375
Set the Optional Management TLVs.....	376
Set the Optional IEEE 802.1 Organizationally-Specific TLVs.....	377
Set the Optional IEEE 802.3 Organizationally-Specific TLVs.....	378
Set the Optional Organizationally Specific TLVs.....	378

Set the LLDP Transmission Parameters to Default Values.....	379
Set the Port Parameters to Default Values.....	380
Set the LLDP MED Policies to Default Values.....	381
Set the LLDP Management TLVs to default values.....	381
Set the Optional IEEE 802.1 and Organize Specific TLVs to Default Values.....	382
Set the Optional IEEE 802.3 and Organize Specific TLVs to Default Values.....	383
Set the Default Values for the Optional TLVs for MED Devices.....	384
Disable LLDP Features on the Port.....	385
Disable LLDP MED Policies for Switch Ports.....	385
Disable the Optional Management TLVs.....	386
Disable the Optional IEEE 802.1 TLVs.....	387
Disable the Optional IEEE 802.3 TLVs.....	387
Disable the Optional LLDP MED TLVs.....	388
View the LLDP Parameters.....	388
View the LLDP Port Parameters.....	390
View the LLDP MED Policy Information.....	393
Configure the PoE Conservation Level Request TLV .....	394
View the Switch PoE Conservation Level Request TLV Configuration.....	395
View PoE Conservation Level Support TLV Information.....	395
Configure the Switch Call Server IP Address TLV .....	396
View the Switch Call Server IP Address TLV Configuration.....	397
View IP Phone Call Server IP Address TLV Information.....	397
Configure the Switch File Server IP Address TLV.....	398
View the Switch File Server IP Address TLV Configuration.....	399
View IP Phone File Server IP Address TLV Information.....	400
Configure the 802.1Q Framing TLV.....	400
View the Switch 802.1Q Framing TLV Configuration.....	401
View IP phone 802.1Q Framing TLV Information.....	402
Configure TLV Transmission Flags.....	402
Display TLV Transmit Flag Status.....	403
Display IP Phone IP TLV Configuration.....	404
LLDP Configuration Example.....	405
Detailed Configuration Commands.....	407
Configuring LLDP using the EDM.....	409
LLDP configuration using EDM.....	409
LLDP Port dot1 configuration using EDM.....	424
LLDP Port dot3 configuration using EDM.....	429
LLDP Port MED configuration using EDM.....	435
<b>Chapter 7: Zero Touch Provisioning Plus (ZTP+)</b> .....	<b>450</b>
ZTP+ Fundamentals.....	450
ZTP+ .....	450
ZTP+ Phases of Operation.....	451
ZTP+ Limitations.....	454



- Configuring ZTP+ using the CLI..... 454
  - View ZTP+ Status..... 454
  - Enable ZTP+..... 454
  - Disable ZTP+..... 455
  - Verify the Firmware Version..... 456
  - Verify DNS Configuration..... 456
  - Verify ZTP+ Auto-provisioning..... 457
  - Enable the DHCP-OOB client..... 459
  - Disable the DHCP-OOB client..... 459
  - Verify IP Settings..... 459
- Configuring ZTP+ Examples..... 460
  - Configure and Manage a Simple ZTP+ Solution..... 460
  - Configure ZTP+ with FA-Provisioned Management VLAN..... 470
- Glossary..... 480**

# Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

---

## Purpose

This document provides instructions to configure the switch software on the following platforms:

- Extreme Networks Ethernet Routing Switch 4900 Series
- Extreme Networks Ethernet Routing Switch 5900 Series

Examples and network illustrations in this document may illustrate only one of the supported platforms. Unless otherwise noted, the concept illustrated applies to all supported platforms.

---

## Conventions




This section discusses the conventions used in this guide.

---

## Text Conventions

The following tables list text conventions that can be used throughout this document.

**Table 1: Notice Icons**

Icon	Alerts you to...
 <b>Important:</b>	A situation that can cause serious inconvenience.
 <b>Note:</b>	Important features or instructions.
 <b>Tip:</b>	Helpful tips and notices for using the product.

*Table continues...*




Icon	Alerts you to...
 <b>Danger:</b>	Situations that will result in severe bodily injury; up to and including death.
 <b>Warning:</b>	Risk of severe personal injury or critical loss of data.
 <b>Caution:</b>	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets ( < > )	<p>Angle brackets ( &lt; &gt; ) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command.</p> <p>If the command syntax is <code>cfm maintenance-domain maintenance-level &lt;0-7&gt;</code>, you can enter <code>cfm maintenance-domain maintenance-level 4</code>.</p>
<b>Bold text</b>	<p>Bold text indicates the GUI object name you must act upon.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• On the <b>Tools</b> menu, choose <b>Options</b>.</li> </ul>
Braces ( { } )	<p>Braces ( { } ) indicate required elements in syntax descriptions. Do not type the braces when you enter the command.</p> <p>For example, if the command syntax is <code>ip address {A.B.C.D}</code>, you must enter the IP address in dotted, decimal notation.</p>
Brackets ( [ ] )	<p>Brackets ( [ ] ) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command.</p> <p>For example, if the command syntax is <code>show clock [detail]</code>, you can enter either <code>show clock</code> or <code>show clock detail</code>.</p>
Ellipses ( ... )	<p>An ellipsis ( ... ) indicates that you repeat the last element of the command as needed.</p> <p>For example, if the command syntax is <code>ethernet/2/1 [ &lt;parameter&gt; &lt;value&gt; ]...</code>, you enter <code>ethernet/2/1</code> and as many parameter-value pairs as you need.</p>

*Table continues...*

Convention	Description
<i>Italic Text</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
Plain Courier Text	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages.  Examples: <ul style="list-style-type: none"><li>• <code>show ip route</code></li><li>• <code>Error: Invalid command syntax</code> <code>[Failed][2013-03-22 13:37:03.303</code> <code>-04:00]</code></li></ul>
Separator ( > )	A greater than sign ( > ) shows separation in menu paths.  For example, in the Navigation tree, expand the <b>Configuration &gt; Edit</b> folders.
Vertical Line (   )	A vertical line (   ) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command.  For example, if the command syntax is <code>access-policy by-mac action { allow   deny }</code> , you enter either <code>access-policy by-mac action allow</code> or <code>access-policy by-mac action deny</code> , but not both.

---

## Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and software compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other resources](#) such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit [www.extremenetworks.com/education/](http://www.extremenetworks.com/education/).

---

## Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

**[Extreme Portal](#)** Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

**[The Hub](#)** A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

**[Call GTAC](#)** For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

### Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to [www.extremenetworks.com/support/service-notification-form](http://www.extremenetworks.com/support/service-notification-form).
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.



**Note:**

You can modify your product selections or unsubscribe at any time.

4. Select **Submit**.

---

## Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at [documentation@extremenetworks.com](mailto:documentation@extremenetworks.com).

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

# Chapter 2: New in this document

The following section details what is new in this document.

## **Zero Touch Provisioning Plus (ZTP+)**

This release introduces support for Zero Touch Provisioning Plus (ZTP+).

Using ZTP+, switches communicate with the Extreme Management Center™ (XMC) as soon as they are connected to the network, allowing them to obtain firmware and configuration updates automatically. This auto-provisioning process significantly minimizes the amount of time required to configure a new switch and deploy it on the network.

For more information, see the following:

- [ZTP+ Fundamentals](#) on page 450
- [Configuring ZTP+ using the CLI](#) on page 454
- [Configuring ZTP+ Examples](#) on page 460

# Chapter 3: System Configuration

This chapter provides conceptual and procedural information related to the configuration and management of system functionality.

---

## System Configuration Fundamentals

This section describes the system configuration fundamentals for the switch.

---

## Feature Licensing

This section describes the types of licenses and lists the features that require a license. Switches and licenses are purchased separately.

You require either an Advanced License or a Trial License to enable certain features. These software licenses support the following features:

- Open Shortest Path First (OSPF)
- Virtual Router Redundancy Protocol (VRRP)
- Equal Cost Multi Path (ECMP)
- Protocol Independent Multicast-Sparse mode (PIM-SM)
- IPv6 Forwarding
- IP Shortcuts
- Routing Information Protocol next generation (RIPng)
- MACSec

You can obtain a trial license to try out advanced license features for 60 days. Trial licenses are obtained from Extreme Networks and installed using the CLI. After the trial period expires, the licensed feature is disabled.

To minimize network and device impacts, the following events occur before the expiration of a trial license:

- A system trap is sent five days before license expiration.
- A system trap is sent one day before license expiration.



- A system trap is sent at license expiration.

License files that have an .xml extension are created using a newer license generator and are considered newer license files. Newer licenses are supported on ERS 4900 and 5900 Series. To obtain a new license, go to the Extreme Networks Support Portal at <https://extremeportal.force.com/ExtrLicenseLanding>.

**\* Note:**

Release 7.5 or later is required to support licenses generated through the Extreme Networks Support Portal.

**! Important:**

The software continues to support .xml licenses generated by Avaya.

If you require a change or regeneration of Avaya-provided licenses, send your email request to: [datalicensing@extremenetworks.com](mailto:datalicensing@extremenetworks.com).

## Hardware features

This section provides information about the hardware features for the following switch platforms:

- Ethernet Routing Switch 4900 Series
- Ethernet Routing Switch 5900 Series

### Ethernet Routing Switch 4900 Series Models

The following table lists the ERS 4900 Series models and the key features for each switch.

**Table 3: ERS 4900 Series models**

Model	Key features	Part Number
ERS 4926GTS	<ul style="list-style-type: none"> <li>• 24 ports, 10/100/1000 Base-T Ethernet with two ports of SFP + (10 Gbps) interfaces</li> <li>• Stackable Ethernet switch</li> <li>• Non-PoE</li> <li>• Supports two modular 250 W Power Supply Units (PSU), where one PSU is required for operation and the optional second is redundant</li> </ul>	AL4900A01-E6 (no power cord)
ERS 4926GTS-PWR+	24 ports 10/100/1000BaseT Stackable Ethernet switch PoE	AL4900A02-E6 (no power cord)

*Table continues...*

Model	Key features	Part Number
	1 rack unit high Uses modular power supply units and has two field-serviceable power supply receptacles, which support 250 W AC power supply modules	
ERS 4950GTS	48 ports 10/100/1000BaseT Stackable Ethernet switch Non-PoE 1 rack unit high Uses modular power supply units and has two field-serviceable power supply receptacles, which support 1025 W AC power supply modules	AL4900A03-E61 (no power cord)
ERS 4950GTS-PWR+	48 ports 10/100/1000BaseT Stackable Ethernet switch PoE 1 rack unit high Uses modular power supply units and has two field-serviceable power supply receptacles, which support 1025 W AC power supply modules	AL4900A04-E6 (no power cord)
Power cords must be ordered separately. Depending on the switch model, a 250 W or 1025 W PSU and .5 m stacking cable is provided for all switches.		

## Ethernet Routing Switch 5900 Series Models

The following table lists the different ERS 5900 Series models and the key features for each switch.

**Table 4: ERS 5900 Series models**

Switch Model	Key features	Part Number
ERS 5928MTS-uPWR	<ul style="list-style-type: none"> <li>• 24x 100/1000/2500Mbps full duplex RJ45 Ethernet User Ports supporting the 802.3at Type II (POE+) Standard and Non-Standard 60 Watts</li> <li>• Four SFP+ 1/10 Gbps uplink ports</li> <li>• Layer 2/Layer 3</li> <li>• Stackable Ethernet switch</li> </ul>	AL590009A-E6GS [no power supply unit (PSU), no power cord (PC)] AL5900A9B-E6GS (no PC) AL5900A9F-E6GS (no PC)

*Table continues...*

Switch Model	Key features	Part Number
	<ul style="list-style-type: none"> <li>• 1 rack unit (U) high</li> <li>• Uses modular power supply units and has two field-serviceable power supply receptacles, which support 1400 W AC power supply modules.</li> </ul>	
ERS 5928GTS	<ul style="list-style-type: none"> <li>• 24 10/100/1000 Base-T RJ-45 ports</li> <li>• Four SFP+ 1/10 Gbps uplink ports</li> <li>• Non-PoE</li> <li>• Layer 2/Layer 3</li> <li>• Stackable Ethernet switch</li> <li>• 1 rack unit (U) high</li> <li>• Uses modular power supply units and has two field-serviceable power supply receptacles, which support 450 W AC power supply modules.</li> </ul>	AL590001A-E6 (no PSU, no PC) AL5900A1B-E6 (no PC) AL5900A1F-E6 (no PC)
ERS 5928GTS-PWR+	<ul style="list-style-type: none"> <li>• 24 10/100/1000 Base-T RJ-45 ports with 802.3at PoE+</li> <li>• Four SFP+ 1/10 Gbps uplink ports</li> <li>• Layer 2/Layer 3</li> <li>• Stackable Ethernet switch</li> <li>• 1 rack unit (U) high</li> <li>• Uses modular power supply units and has two field-serviceable power supply receptacles, which support 1400 W AC power supply modules.</li> </ul>	AL590002A-E6 (no PSU, no PC) AL5900A2B-E6 (no PC) AL5900A2F-E6 (no PC)
ERS 5928GTS-uPWR	<ul style="list-style-type: none"> <li>• 24 10/100/1000 Base-T RJ-45 ports with 802.3at PoE+</li> <li>• Four SFP+ 1/10 Gbps uplink ports</li> <li>• Layer 2/Layer 3</li> <li>• Stackable Ethernet switch</li> <li>• 1 rack unit (U) high</li> </ul>	AL5900A7A-E6 (no PSU, no PC) AL5900A7B-E6 (no PC) AL5900A7F-E6 (no PC)

*Table continues...*

Switch Model	Key features	Part Number
	<ul style="list-style-type: none"> <li>• Uses modular power supply units and has two field-serviceable power supply receptacles, which support 1400 W AC power supply modules.</li> </ul>	
ERS 5952GTS	<ul style="list-style-type: none"> <li>• 48 10/100/1000 Base-T RJ-45 ports</li> <li>• Four SFP+ 1/10 Gbps uplink ports</li> <li>• Non-PoE</li> <li>• Layer 2/Layer 3</li> <li>• Stackable Ethernet switch</li> <li>• 1 rack unit (U) high</li> <li>• Uses modular power supply units and has two field-serviceable power supply receptacles, which support 450 W AC power supply modules.</li> </ul>	AL590003A-E6 (no PSU, no PC) AL5900A3B-E6 (no PC) AL5900A3F-E6 (no PC)
ERS 5952GTS-PWR+	<ul style="list-style-type: none"> <li>• 48 10/100/1000 Base-T RJ-45 ports with 802.3at PoE+</li> <li>• Four SFP+ 1/10 Gbps uplink ports</li> <li>• Layer 2/Layer 3</li> <li>• Stackable Ethernet switch</li> <li>• 1 rack unit (U) high</li> <li>• Uses modular power supply units and has two field-serviceable power supply receptacles, which support 1400 W AC power supply modules.</li> </ul>	AL590004A-E6 (no PSU, no PC) AL5900A4B-E6 (no PC) AL5900A4F-E6 (no PC)
ERS 59100GTS	<ul style="list-style-type: none"> <li>• 96 10/100/1000 Base-T RJ-45 ports</li> <li>• Four SFP+ 1/10 Gbps uplink ports</li> <li>• Stackable Ethernet switch</li> <li>• Layer 2/Layer 3</li> <li>• Non-PoE</li> <li>• 1 rack unit (U) high</li> </ul>	AL5900A5A-E6 (no PSU, no PC) AL5900A5B-E6 (no PC) AL5900A5F-E6 (no PC)

*Table continues...*

Switch Model	Key features	Part Number
	<ul style="list-style-type: none"> <li>• Uses modular power supply units and has four field-serviceable power supply receptacles, which support 450 W AC power supply modules.</li> </ul>	
ERS 59100GTS-PWR+	<ul style="list-style-type: none"> <li>• 96 10/100/1000 Base-T RJ45 ports with 802.3at PoE+</li> <li>• Four SFP+ 1/10 Gbps uplink ports</li> <li>• Layer 2/Layer 3</li> <li>• Stackable Ethernet switch</li> <li>• 1 rack unit (U) high</li> <li>• Uses modular power supply units and has four field-serviceable power supply receptacles, which support 1400 W AC power supply modules.</li> </ul>	AL5900A6A-E6 no PSU, no PC) AL5900A6B-E6 (no PC) AL5900A6F-E6 (no PC)
<p>Power cords must be ordered separately.</p> <p><b>* Note:</b>            The 'B' in the part number (for example, AL5900E4B-E6) denotes Back to Front cooling, whereas 'F' denotes Front to Back cooling (for example, AL5900E4F-E6).</p>		

## Cooling fans

ERS 5900 Series switches support two field-replaceable fan trays and ERS 59100 support four field-replaceable fan trays for switch cooling.

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

**\* Note:**

ERS 4900 does not support cooling fans.

For more information about installation, see [Installing Ethernet Routing Switch 5900 Series](#).

---

## Stacking Capabilities

You can use the switches in either of the following configurations:

- stand-alone
- stack

The switches have a built-in cascade port to stack up to eight units. The cascade port provides a 40 gigabit (Gb) cascading mechanism for the stacks.

A stack can consist of any combination of switches from the same switch series.

**\* Note:**

You can stack only four units of ERS 59100GTS or ERS 59100GTS-PWR+.

**! Important:**

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

To set up a stack, perform the following procedure:

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

---

## Auto Unit Replacement

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

The main feature of the AUR is the ability to retain the configuration (CFG) image of a unit in a stack during a unit replacement. In a non-based unit (NBU) replacement, the retained CFG image from the old unit is restored to the new unit. In a base-unit (BU) replacement, the CFG image of the BU is saved in the NBU and the CFG of the NBU is saved in the BU. Because retained CFG images are kept in the Dynamic Random-Access Memory (DRAM) of the stack, the stack power must be on during the procedure.

**! Important:**

For Auto Unit Replacement to function properly, the new unit and the existing units in the stack must all run the same version of software.

You can manually restore an associated configuration (same unit number) of a unit in a stack including base unit.

**! Important:**

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

### Limitations

While replacing the base unit, ensure to check the following:

- 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 configuration of this unit is used.
- If you add a new unit with the same hardware configuration, the previous configuration of the new unit is lost. The configuration is overwritten with the restored configuration from the stack.
- You can enable or disable this feature at any time using CLI. The default mode is Enable.
- Log messages are provided.

After installing the AUR and AAUR enhancement for base unit in two high stack, you cannot manually restore AUR on the base unit. Perform any of the following steps to restore the settings depending on the scenario:

- Save the configuration using the following command:

```
stack-auto unit replacement config save unit <id>
```

**\* Note:**

The configuration cannot be restored for base unit.

- If the unit previously belonged to a different stack, power recycle the replacement unit before adding it to the stack.
- If the base unit is replaced with another unit that runs a different software image, the image must have AUR and AAUR two high stack enhancement. The reason is, replacement unit gets the image from the non-base unit.

If the software image is different in the replacement base unit and the image does not contain the AUR and AAUR two high stack enhancement, then AAUR behaves prior to this enhancement (non-base unit gets the image from the new base unit).

## AUR function

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

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

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

## CFG mirror image process

The CFG mirror image process is triggered by specific events such as:

- A power cycle
- Adding a unit
- Removing a non-base unit (NBU)
- Removing a base unit (BU)
- Restoring a CFG image

- Synchronizing with a CFG flash drive in the AU

### Power Cycle

After a power cycle, all the CFG images in a stack are mirrored. [Figure 1: CFG mirror process in stack](#) on page 24 illustrates the CFG mirror images in a three-unit stack after the stack is powered on. Unit 1 is the Base Unit (BU) and all other units are Non-Base Units (NBU).

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

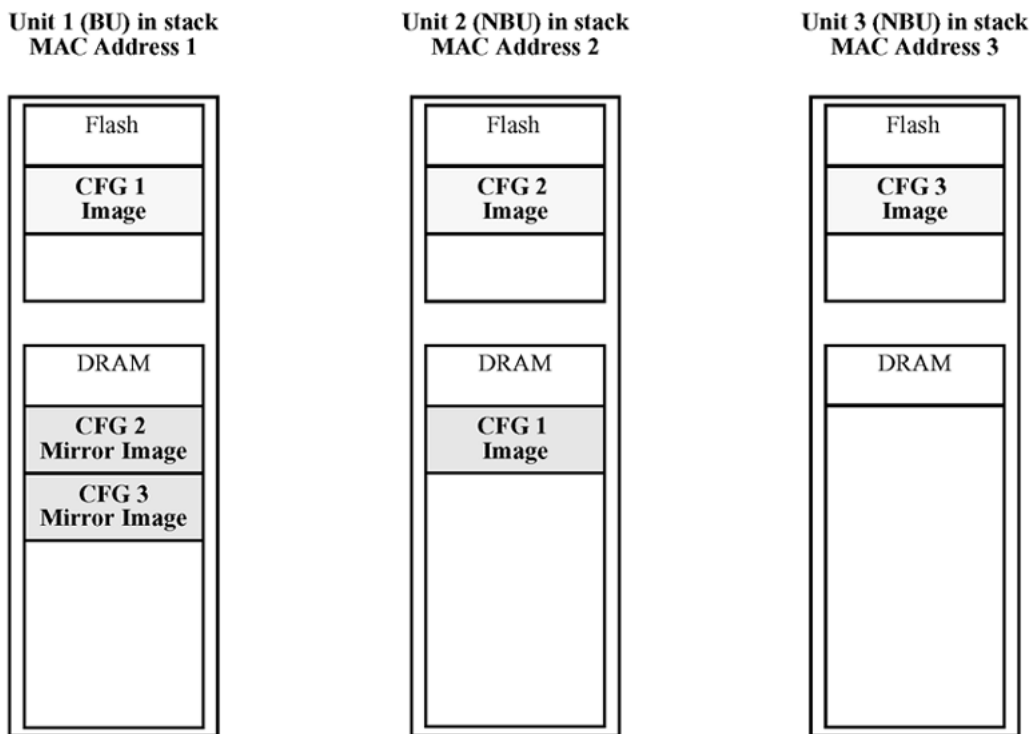
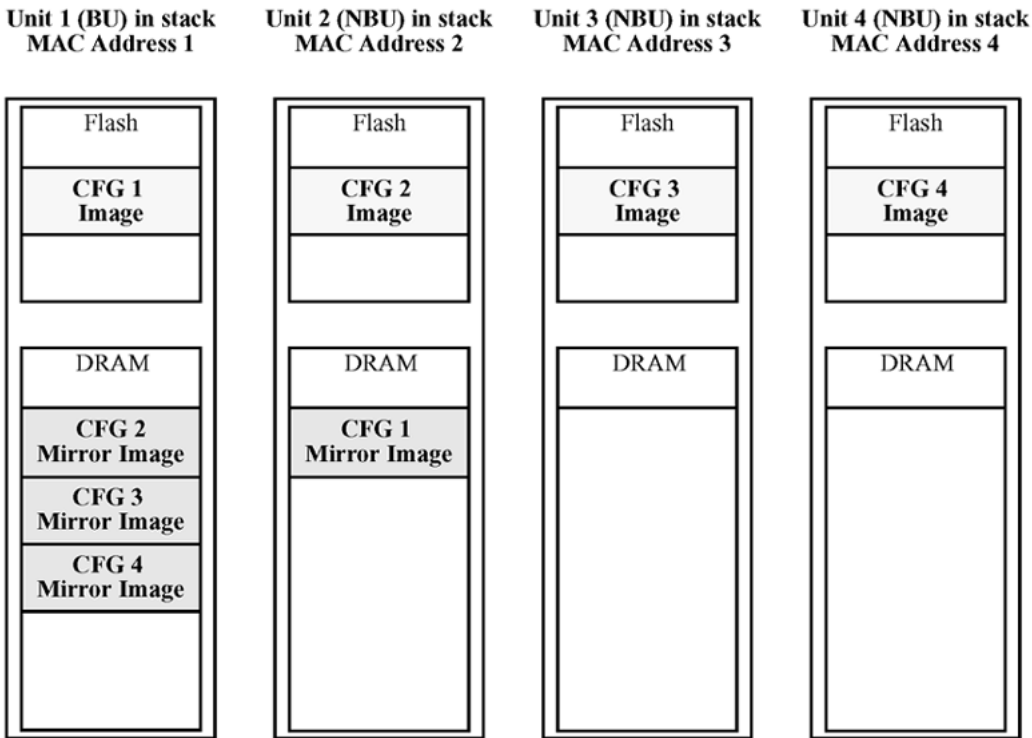


Figure 1: CFG mirror process in stack

### Adding a unit

In a stack that has no INACTIVE CFG mirror images, a new unit causes the CFG image of the new unit to be mirrored in the stack. For example, in [Figure 2: CFG mirror images in the stack after adding unit 4](#) on page 25, after you add unit 4 to the stack, the CFG 4 mirror image is created in the BU (unit 1).





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

## Removing an NBU

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

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

For example, after you remove unit 4 from the stack shown in [Figure 2: CFG mirror images in the stack after adding unit 4](#) on page 25, the CFG 4 mirror image becomes INACTIVE (see [Figure 3: CFG mirror images after removing unit 4](#) on page 26). Another copy of the INACTIVE CFG 4 mirror image is also created in unit 2.

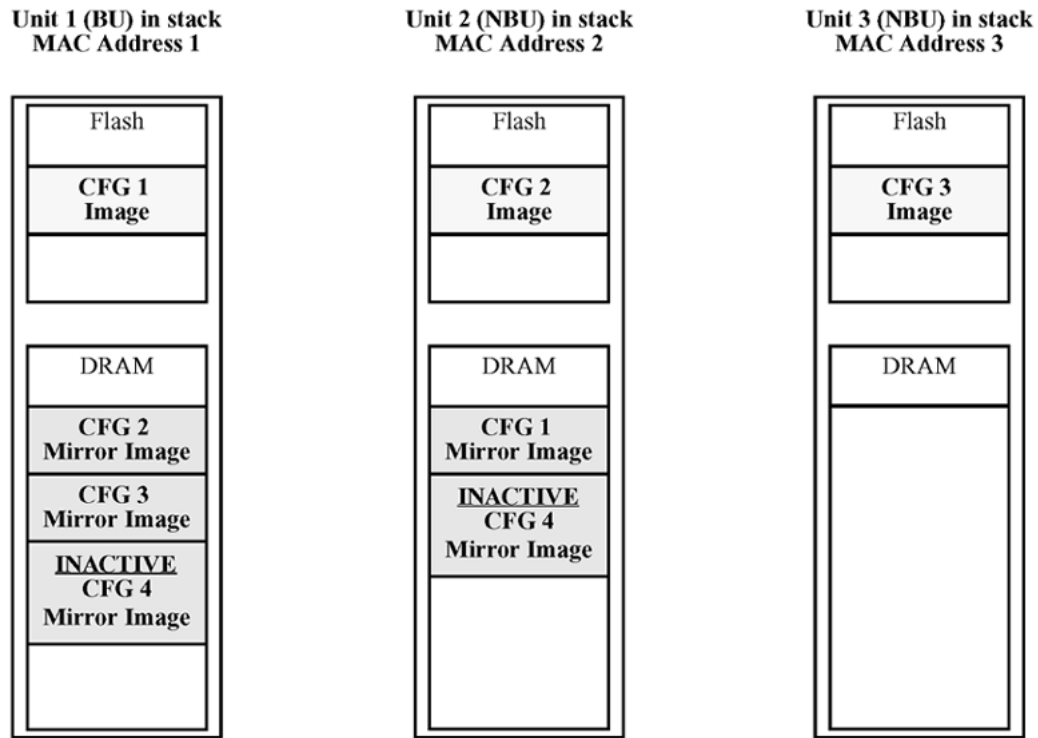
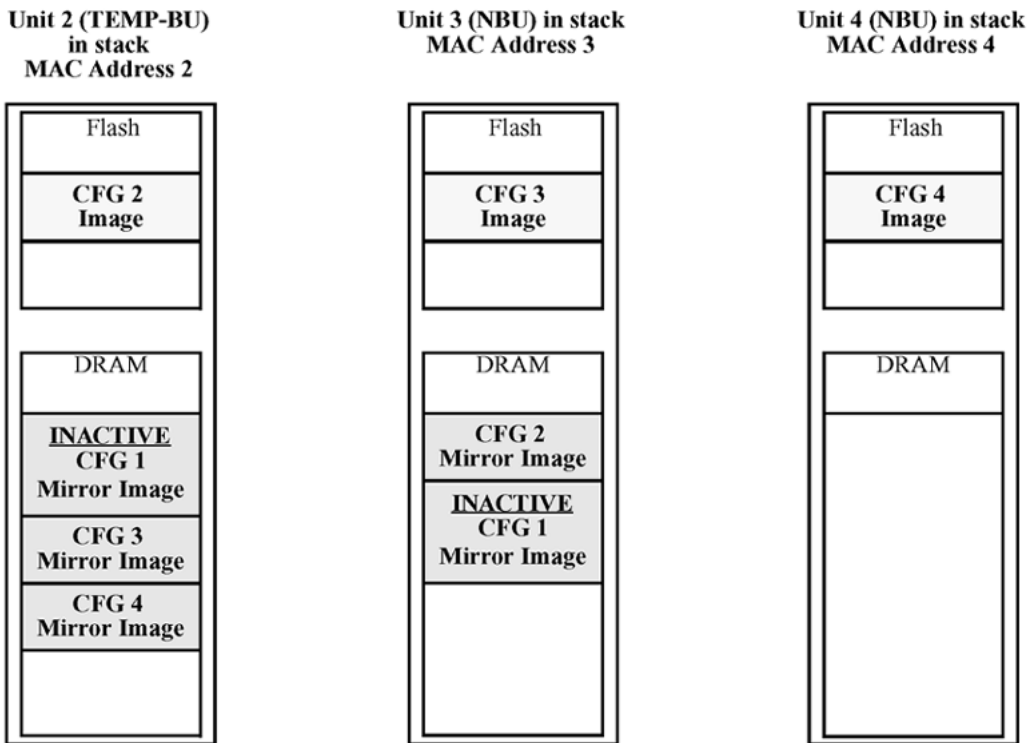


Figure 3: CFG mirror images after removing unit 4

### Removing a BU

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

After you remove the BU from the stack shown in [Figure 2: CFG mirror images in the stack after adding unit 4](#) on page 25, the TEMP-BU (unit 2) must mirror all the CFG images in the stack (see [Figure 4: CFG mirror images in the stack after removing the BU \(unit 1\)](#) on page 27). The feature also ensures that the stack always has two copies of an INACTIVE CFG mirror image.



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

As shown in [Figure 4: CFG mirror images in the stack after removing the BU \(unit 1\)](#) on page 27:

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

### Restoring a CFG Image

When you restore a CFG image, the system overwrites the CFG image of a new unit in a stack with an INACTIVE mirror image stored in the stack.

#### ! Important:

You can restore a CFG image to a new unit happens only if you meet the following conditions:

- The AUR feature is enabled.
- At least one INACTIVE CFG mirror image exists in the stack.

- The MAC address of the new unit is different from all the AMA of the INACTIVE CFG mirror images in the stack.

When you add a new unit to a stack, the image restore process consists of the following steps.

1. If more than one INACTIVE CFG mirror image is in the stack, select the one with the smallest unit ID for restoration.
2. Send the INACTIVE CFG mirror image in the stack to the new unit. The INACTIVE CFG mirror image becomes ACTIVE.

The new unit saves the received CFG image to the flash drive and resets itself.

For example, if you add a unit 5 (MAC address 5) to the stack shown in [Figure 4: CFG mirror images in the stack after removing the BU \(unit 1\)](#) on page 27, the following occurs (see [Figure 5: CFG mirror images in the stack after adding unit 5](#) on page 28):

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

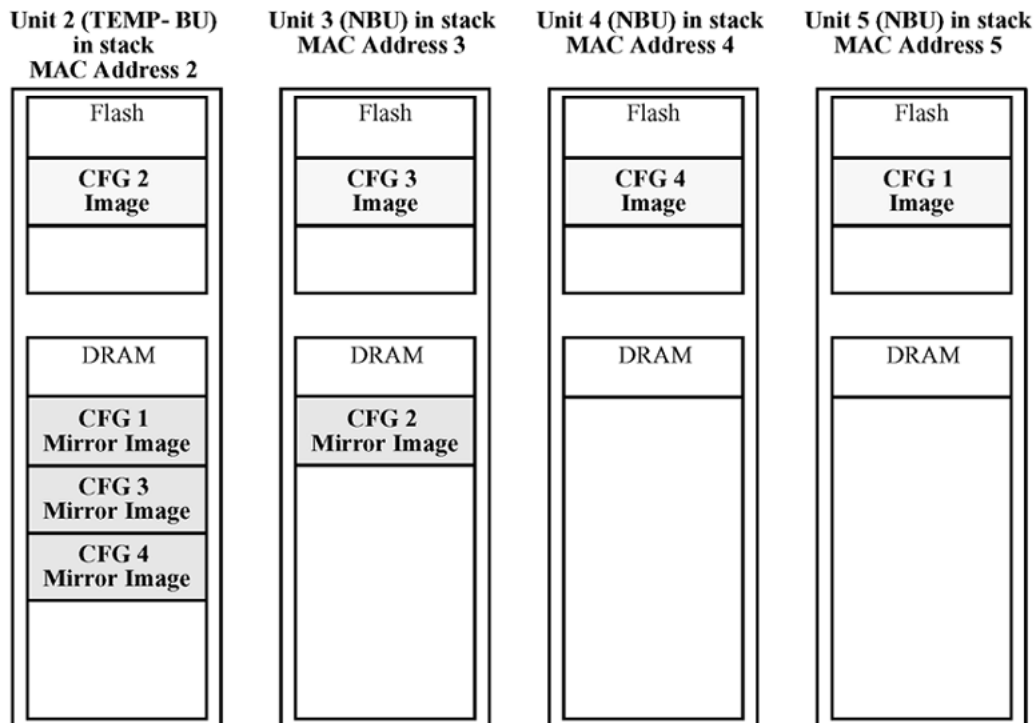


Figure 5: CFG mirror images in the stack after adding unit 5

## Synchronizing the CFG mirror images with CFG images

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

## Agent Auto Unit Replacement

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

Agent Auto Unit Replacement functions in the following manner:

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

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

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

```
I 2 00:01:56:48 14 AAUR - Info: Agent transfer finished
```

---

## Diagnostic Auto Unit Replacement

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

DAUR updates the diagnostic image on added units in the same way that AAUR updates the agent software.

In an AAUR-enabled stack, the DAUR process starts if a unit with a different diagnostic image is connected to the stack. This process updates all the units in the stack.

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

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

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

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

---

## 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.

See [Configuring Stack Forced Mode](#) on page 128 or [Configuring system parameters using EDM](#) on page 251 for procedures to configure the Stack Forced Mode on a switch.

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

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

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

When a failure occurs in a stack of two units when Stack Forced Mode is enabled, the previous non-base unit sends out a gratuitous ARP onto the management network so that the non-base unit of a failed two-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 two units in a stack were connected by a single stack cable and that stack cable were then removed or failed. If the previous non-base unit receives a reply from the previous base unit of the stack, the previous non-base unit knows that the previous base unit is still operational and does not take over ownership of the stack IP address, but instead uses 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 now takes over ownership of the stack IP address and issues a gratuitous ARP with its own MAC address. This ensures 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 Forced Mode and you want to set a switch IPv6 address, you must first delete the active IPv6 interface and then configure the switch IPv6 address. If you use telnet, SSH or EDM to change the settings, the switch loses IPv6 connectivity to the switch. Extreme Networks recommends that you change the settings with the Console Interface to the switch or use an IPv4 address for management.

---

## IPv6 Management

This section provides information about the IPv6 Management feature of the switch platform.

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

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.

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

### The IPv6 header

The IPv6 header contains the following fields:

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

### IPv6 addresses

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

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

[Figure 6: IPv6 address format](#) on page 32 shows the IPv6 address format.

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

**Figure 6: IPv6 address format**

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

## Interface ID

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

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

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

## Address formats

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

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

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

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

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

An IPv4-compatible address combines hexadecimal and decimal values as follows:

x:x:x:x:x: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

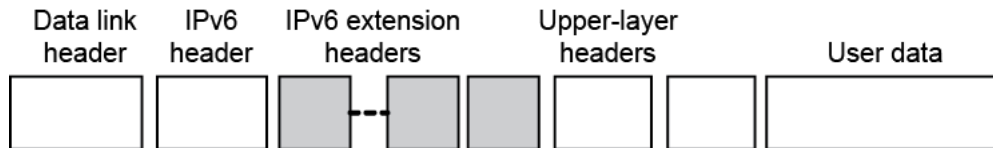
or

::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. For more information, see [Figure 7: IPv6 header and extension headers](#) on page 33.





**Figure 7: IPv6 header and extension headers**

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

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

IPv6 defines the following extension headers:

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

## Comparison of IPv4 and IPv6

The following table compares key differences between IPv4 and IPv6.

**Table 5: IPv4 and IPv6 differences**

Feature	IPv4	IPv6
Address length	32 bits	128 bits
IPsec support <sup>1</sup>	Optional	Required
QoS support	Limited	Improved
Fragmentation	Hosts and routers	Hosts only
Minimum MTU (packet size)	576 bytes	1280 bytes
Checksum in header	Yes	No
Options in header	Yes	No

*Table continues...*

Feature	IPv4	IPv6
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	Manual, DHCP	Manual, AAA, DHCPv6
<sup>1</sup> The switch does not support IPsec.		
<sup>2</sup> The switch does not perform Router discovery or advertise as a router.		

## ICMPv6

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

### Important:

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

## Neighbor discovery

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

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

Neighbor discovery protocol provides you with the following:

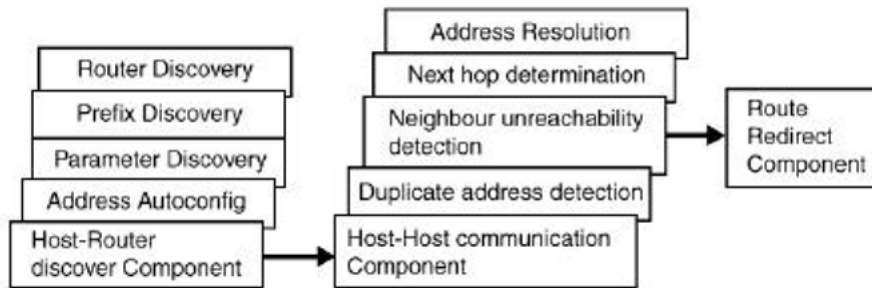
- Address and prefix discovery: hosts determine the set of addresses that are on-link for the given link. Nodes determine which addresses or prefixes are locally reachable or remote with address and prefix discovery.
- Router discovery: hosts discover neighboring routers with router discovery. Hosts establish neighbors as default packet-forwarding routers.
- Parameter discovery: host and routers discover link parameters such as the link MTU or the hop limit value placed in outgoing packets.
- Address autoconfiguration: nodes configure an address for an interface with address autoconfiguration.
- Duplicate address detection: hosts and nodes determine if an address is assigned to another router or a host.

- Address resolution: hosts determine link layer addresses (MAC for Ethernet) of the local neighbors (attached on the local network), provided the IP address is known.
- Next-hop determination: hosts determine how to forward local or remote traffic with next-hop determination. The next hop can be a local or remote router.
- Neighbor unreachability detection: hosts determine if the neighbor is unreachable, and address resolution must be performed again to update the database. For neighbors you use as routers, hosts attempt to forward traffic through alternate default routers.
- Redirect: routers inform the host of more efficient routes with redirect messages.

Neighbor discovery uses three components:

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

For more information, see [Figure 8: Neighbor discovery components](#) on page 35 for the ND components.



**Figure 8: Neighbor discovery components**

## ND Messages

The following table shows new ICMPv6 message types.

**Table 6: IPv4 and IPv6 neighbor discovery comparison**

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

*Table continues...*

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

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

- **Static:** a configured neighbor
- **Local:** a device on the local system
- **Dynamic:** a discovered neighbor

The following table describes neighbor cache states.

**Table 7: Neighbor cache states**

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

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

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

## Router discovery

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

- Router advertisement
- Router solicitation

## Router advertisement

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

## Router solicitation

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

## Path MTU discovery

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

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

The default MTU value for a regular interface is 1500.

## IPv6 First Hop Security

IPv6 is expected to coexist with and eventually replace IPv4. In most of the networks, IPv6 is increasingly getting deployed and success of the deployment depends on the network security and Quality of Service (QoS) that it offers compared to IPv4.

Enhancements in IPv6 provides security in certain areas, but some of these areas are still open to exploitation by the attackers. The attack can be address theft, spoofing, and remote address resolution cache exhaustion (denial of service attacks). These security breaches can severely disrupt Layer 2 domains and networks in general. IPv6 First Hop Security (FHS) solution protects networks by mitigating these types of attacks.

First Hop Security contains the majority of the RIPE 554 mandatory requirement for Layer 2 switches. This includes the following:

- DHCPv6-guard
- Router Advertisement guard
- Dynamic IPv6 Neighbor solicitation or advertisement inspection
- Neighbor Unreachability Detection inspection
- Duplicate Address Detection inspection
- IPv6 Source Guard

For more information about First Hop Security, see [Configuring Security on Ethernet Routing Switch 4900 and 5900 Series](#).

---

## Jumbo frames

Jumbo frames are Ethernet frames larger than the maximum Ethernet frame size, or maximum transmission unit (MTU) specified in the IEEE 802.3 standard. For untagged frames, the maximum standard size is 1518 bytes. For tagged frames, the maximum standard size increases by 4 bytes to 1522 bytes.

Enabling jumbo frames on a switch sets the MTU size to 9216 bytes (9220 bytes for tagged frames). By default, the jumbo frames are enabled.

Jumbo frames are used to improve network throughput and decrease CPU load. The following are the benefits when jumbo frames are enabled:

- Each frame carries a larger payload as the header sizes remain the same.
- There are fewer interrupts on the server due to fewer frames and a smaller CPU load.
- Larger frames provide better buffer utilization and forwarding performance in switches.

---

## Flash memory storage

The following sections describe flash memory for software image upgrades.

### Switch Software Image Storage

The switch software image storage uses FLASH memory to store the switch software image.

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

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

#### Important:

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

### Configuration parameter storage

All configuration parameters in the configuration parameter storage are stored in FLASH memory.

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

#### Important:

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

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

## Show FLASH

The Show FLASH feature displays information about the FLASH capacity and current usage, including:

- Total FLASH capacity
- Size and version of boot image
- Size and version of agent image
- Size and version of diagnostic image
- Size and version of secondary agent image (if supported)
- Size of binary configuration
- Size of automatic backup configuration
- Size of secondary configuration
- Size of reserved space on FLASH
- Size of available space on FLASH

This feature is available on both single and stacked switches.

## Show FLASH History

The Show FLASH History feature displays information about the number of writes or modification to the following sections:

- Diagnostics Image
- Primary Image
- Secondary Image
- Configuration Area 1
- Configuration Area 2
- Auxiliary Configuration Area
- MCFG Block
- Audit Log Area

**\* Note:**

Recording of FLASH history begins after installing or upgrading the switch to a release with this feature. FLASH events that occurred prior to the release remain unknown.

---

## Policy-enabled networking

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



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

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

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

---

## Port Mirroring

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

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

For more information about port mirroring, see [Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series](#).

### Important:

Use CLI to configure port mirroring.

---

## Rate Limiting

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

When the volume of either packet type is high, placing severe strain on the network (often referred to as a storm), you can set the ingress rate of those packet types to not exceed a specified percentage of the total available bandwidth or a specified number of packets per second.

Rate Limiting counts packets from the beginning of each second. When the number of packets reaches the value of the rate limit, all remaining packets are dropped until the end of the second. As a result, the packets are not evenly distributed over the course of a second. For this reason, rate limiting utilization counters/calculations can appear to be inaccurate.

### Note:

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

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

### Clarification of behavior

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

#### \* Note:

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

The actual traffic received rate received during the following scenarios:

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

The client port will receive  $0.1 * (\text{inbound traffic rate})$  and not the expected 1 Gbps broadcast or multicast traffic. Following is an example:

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

The actual client traffic received rate =  $(0.1 * 3 \text{ Gbps})$  and not the expected 1 Gbps.

---

## Auto-MDI/X

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

When auto-MDI/X is active, straight or crossover Cat5 cables can provide connection to a port. If autonegotiation is disabled, auto-MDI/X is not active.

---

## Auto-polarity

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

With autonegotiation enabled, auto-polarity automatically reverses the polarity of a pair of pins from positive to negative or negative to positive. This corrects the polarity of the received data, if the port detects that the polarity of the data is reversed due to a wiring error. If autonegotiation is disabled, auto-polarity is not active.

---

## Time Domain Reflectometer

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

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

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

The TDR cannot test fibre-optic cables.

---

## Autosensing and Autonegotiation

The switches are autosensing and autonegotiating devices:

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

Autosensing occurs when the attached device cannot autonegotiate or uses a form of autonegotiation that is not compatible with the IEEE 802.3z autonegotiation standard. If it is not possible to sense the duplex mode of the attached device, the switch reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the switch, the ports negotiate down from 10000 Mb/s and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

### **Note:**

If you connect ERS 4900 Series and ERS 5900 Series with VSP 8000 Series, you must disable autonegotiation on the SFP+ port on the ERS 4900 Series and ERS 5900 Series in order to get a 1 Gbit fiber link. This is because the VSP 8000 Series is limited to work only with autonegotiation disabled on 1 Gbit fiber while the default setting for the ERS 4900 Series and ERS 5900 Series is autonegotiation enabled when using 1 Gbit fiber transceivers.

---

## Custom AutoNegotiation Advertisement (CANA)

Custom AutoNegotiation Advertisement offers improved control over the autonegotiation process. The system advertises all port capabilities that include 10 Mb/s, 100 Mb/s, 1000 Mb/s, 2500 Mb/s, 10000 Mb/s speeds, and duplex and half-duplex modes of operation. This advertisement results in autonegotiation between the local and remote end that settles on the highest common denominator. Custom AutoNegotiation Advertisement can advertise a user-defined subset of the capabilities that settle on a lower or particular capability.

---

## Oversubscription and 2.5 Gbps support

Oversubscription occurs when traffic that needs to exit the unit on a port exceeds available bandwidth.

If oversubscription occurs on a 1 Gb port of a 5928MTS unit, pause frames will be seen on show port-statistics output in the *Received* section and *Dropped On No Resources* in the *Transmitted* section. Pause frames are not sent or received on that port and do not influence traffic behavior. They only have internal port meaning. Lossless functionality is not supported.

Oversubscription on 1 Gb or 2.5 Gb port will not equally load balance all traffic from one queue if high drop precedence is used. Not all the flows will have equally load balanced bandwidth at egress in oversubscription case. Equally load balance can be achieved using low drop precedence. For example all traffic will be considered best effort in default qos untrusted group (using default QoS and VLAN priority settings). All flows will be assigned to the same queue with high drop precedence. To set low drop precedence for best effort (untrusted qos group of ports), use the following command: `qos egressmap ds 0 lp 0 dp low-drop`.

---

## ASCII Configuration File

With the ASCII configuration file, you can download a user editable ASCII configuration file from a USB, TFTP or SFTP server.

Use the following sequence at the beginning of the ASCII file:

```
enable
configure terminal
```

### Important:

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

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

## CLI Command Syntax

```
Switch#script ?
```

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

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

After you download the file, the configuration file automatically configures the switch or stack according to CLI 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 CLI.

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

## Sample ASCII Configuration File

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

The following text represents a sample ASCII configuration file:

```
! -----
! example script to configure different features from CLI
! -----
!
enable
configure terminal
!
! -----
! add several MLTs and enable
! -----
mlt 3 name seg3 enable member 13-14
mlt 4 name seg4 enable member 15-16
mlt 5 name seg5 enable member 17-18
!
! -----
! add vlans and ports
! -----
!
! create vlan portbased
vlan create 100 name vlan100 type port
!
! add Mlts created above to this VLAN
vlan members add 100 17
!
! create vlan ip protocol based
vlan create 150 name vlan150 type protocol-ipEther2
!
! add ports to this VLAN
! in this case all ports
```

## System Configuration

```
vlan members add 150 ALL
vlan ports ALL priority 3
!
! igmp
! you could disable proxy on vlan 100
vlan igmp 100 proxy disable
!
! -----
! Examples of changing interface parameters
! -----
! change speed of port 3
interface ethernet 3
speed 10
exit
!
! change speed of port 4
interface ethernet 4
speed auto
exit
!
! -----
! SNMP configuration
! -----
snmp-server host 192.168.100.125 private
snmp-server community private
!
!
exit
end
! -----
! Finished
! -----
```

### Important:

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

## ASCII Download Log

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

### 1. Connection error (ACG\_DOWNLOAD\_ERROR)

The message describes the situation in which the connection failed, therefore the ASCII Configuration File could not be accessed or used. The IP address and the file name are in the message in case of a TFTP server usage, or the file name in case of a USB usage. The message also contains the cause of the error (the same as the one displayed to the CLI). An ACG\_DOWNLOAD\_ERROR error message is logged only in the following situations:

- Transfer Timed Out
- Invalid TFTP Server address
- File not found
- Configuration failed
- Switch IP address not set

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

**\* Note:**

It does not matter from which interface you start the ASCII file download; the logged messages are the ones from the CLI.

**Example message for TFTP server usage:**

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

**Example message for USB usage:**

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

2. Connection error on load on boot (ACG\_DOWNLOAD\_ERROR\_ON\_BOOT)

The message describes the situation in which the connection failed at load on boot; the ASCII Configuration File could not be accessed or used. The IP address and the file name are in the message in case of TFTP server usage, or the file name in case of USB usage. The message also contains the cause of the error ( the same as the one displayed to the CLI). If the IP number is unknown, the question mark (?) is used.

**Example message for TFTP server usage:**

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

**Example message for USB usage:**

```

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

3. Connection OK (ACG\_DOWNLOAD\_OK)

The message describes the situation in which the connection was successful; the ASCII Configuration File could be accessed and used. The IP address and the file name are in the message in case of TFTP server usage, or the file name in case of USB usage.

**Example message for TFTP server usage:**

```

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

**Example message for USB usage:**

```

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

4. Connection OK on load on boot (ACG\_DOWNLOAD\_OK\_ON\_BOOT)

The message describes the situation in which the connection was successful at load on boot; the ASCII Configuration File could be accessed and used. The IP address and the file name are in the message in case of TFTP server usage, or the file name in case of USB usage.

**Example message for TFTP server usage:**

```

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

**Example message for USB usage:**

```

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



### 5. Execution OK (ACG\_EXECUTION\_OK)

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

**Example message for both TFTP server usage and USB usage:**

```

Type          Unit      Time          Idx Src      Message
---- I       ---- 1      -----      ----- 10  ----- ASCII
                                00:00:00:45                                finished successfully.

```

### 6. Execution OK on load on boot (ACG\_EXECUTION\_OK\_ON\_BOOT)

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

**Example message for both TFTP server usage and USB usage:**

```

Type          Unit      Time          Idx Src      Message
---- I       ---- 1      -----      ----- 10  ----- ASCII
                                00:00:00:45                                finished successfully at
                                                load on boot.

```

### 7. Failed command (ACG\_CMD\_ERR)

The message describes the situation in which a command from the ASCII Configuration File failed. The failed command text line number is in the message. If the cause of the error is one of the following, the cause is also given in the message: "Invalid input detected," "Ambiguous command," "Incomplete command," "Permission denied," "Not allowed on slave." In other words, if one of these messages is displayed in the CLI, it is in the ASCII\_CMD\_ERR message.

**\* Note:**

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

**Example error message:**

```

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

```

---

## Backup configuration file

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

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

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

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

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

---

## Booting with an ASCII Configuration File from the Local System

This feature allows you to download an ASCII configuration file from a TFTP server or USB to the local file system and boot the system with the local ASCII configuration file. Two ASCII configuration files are supported, one in each block. When you download and save an ASCII configuration file to the local file system, the system deletes the old file in that block.

The maximum size of an ASCII configuration file is limited to 500 kilobytes.

Once the system boots successfully with an ASCII configuration file, the system configuration is saved to the binary configuration. If the boot fails, the system resets and boots with the current binary configuration.

### Note:

Downgrading software from one major release to another (for example: Release 7.1 to 7.0 ) deletes all the ASCII files from the local ASCII file system, whereas downgrading from a minor release to another minor release (for example: Release 7.1.2 to 7.1.1) does not delete the ASCII files.

Additionally, using the **boot default** command does not delete the ASCII files from the ASCII file system.

---

## Displaying unit uptime

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

---

## Port naming

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

Use CLI or EDM to name ports.

---

## Port error summary

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

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

---

## IP address for each unit in a stack

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

---

## BootP automatic IP Configuration and MAC Address

The switch supports the Bootstrap protocol (BootP).

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

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

The switch 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 switch BootP requests.

The BootP modes supported by the switch are:

- BootP or Last Address mode
- BootP, DHCP or Default IP mode.
- BootP Always
- BootP Disabled

### Important:

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

- Always
- Disabled
- Last
- Default-ip

## Default BootP setting

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

---

## DHCP client

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

---

## Web Quick Start

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

This feature is supported only by the Web interface.

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

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

- Stack IP address
- Subnet mask
- Default gateway
- SNMP Read community
- SNMP Write community
- Quick Start VLAN

---

## Simple Network Time Protocol

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

Use SNTP to provide a real-time timestamp for the software, shown as Greenwich Mean Time (GMT).

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

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

For more information, see [Using Simple Network Time Protocol](#) on page 174.

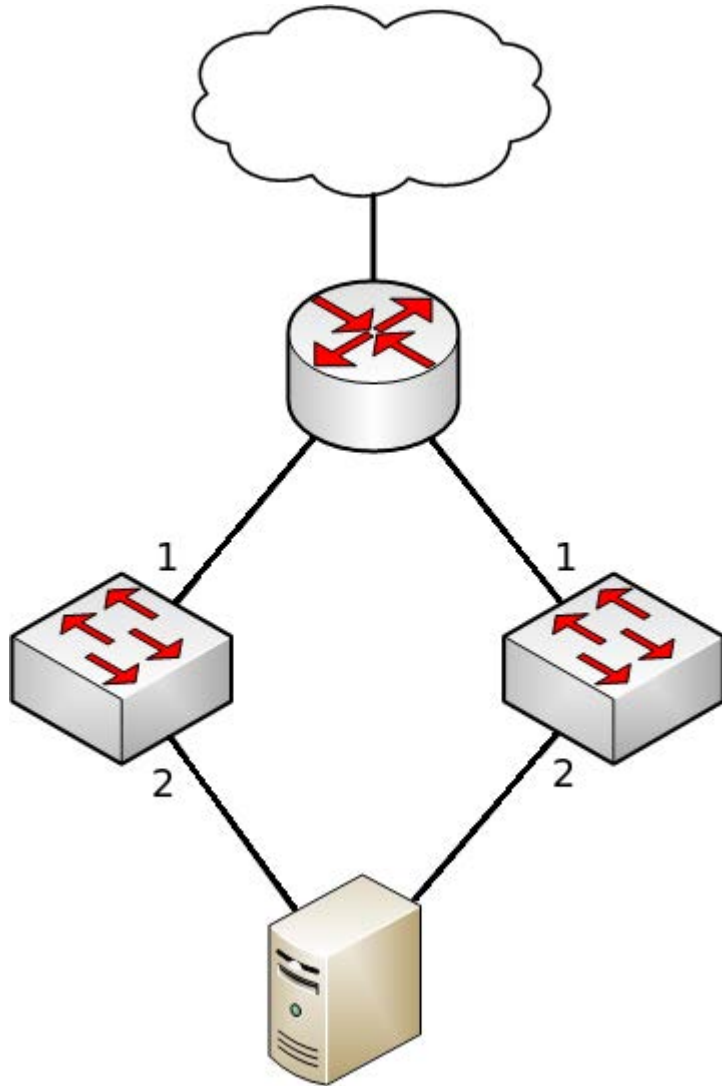
---

## Link-state tracking

Link-state tracking (LST) binds the link state of multiple interfaces. The Link-state tracking feature identifies the upstream and downstream interfaces. The associations between these two interfaces form a link-state tracking group.

To enable link-state tracking, create a link-state group, and specify the interfaces that are assigned to the link-state group. An interface can be an aggregation of ports, multi-link trunks (MLT) or link aggregation groups (LAG). In a link-state group, these interfaces are bundled together. The downstream interfaces are bound to the upstream interfaces. Interfaces connected to servers are referred to as downstream interfaces, and interfaces connected to distribution switches and network devices are referred to as upstream interfaces.

For example, in an application, link-state tracking can provide redundancy in the network with two separate switches or stacks when used with server NIC adapter teaming. The following diagram is a sample scenario. If interface 1 is unavailable on either switch, the server continues to send traffic through interface 2 and the traffic is dropped. If interfaces 1 and 2 are coupled in a link-state group (as upstream and downstream ports respectively), when interface 1 is unavailable, interface 2 is disabled, prompting the server to choose the other path as the target.



**Figure 9: Sample scenario for link-state tracking**

In a link-state group, the upstream ports become unavailable or lose connectivity when the Virtual Link Aggregation Control Protocol (VLACP) is disabled, cables are disconnected, or the link is lost.

The following are the interactions between the downstream and upstream interfaces when link-state tracking is enabled:

- If any of the upstream interfaces are in link-up state, the downstream interfaces are in link-up state.
- If all of the upstream interfaces become unavailable, link-state tracking automatically disables the downstream interfaces.

The following table provides an overview about the link-state feature interactions with other features:

Feature	Interaction
Interface link status	<p>The <code>show interface</code> command displays the link status for ports or trunk members.</p> <p>For upstream interfaces with VLACP disabled, the link status is identical to the one kept by link-state tracking. A port with a link and a trunk with at least one link among its members are considered up.</p>
Interface administrative status	<ul style="list-style-type: none"> <li>• An administrator can enable or disable interfaces that are in the link-state tracking downstream set by issuing <code>shutdown</code> or <code>no shutdown</code> commands.</li> <li>• Link-state tracking does not enable ports which are administratively disabled.</li> <li>• If a port is disabled by link-state tracking, an administrator cannot enable the port and only the administrative status changes. The port can be recovered either by LST (convergence) or by removing the port from the downstream set.</li> </ul>
STP BPDU-Filtering, Mac Security	<ul style="list-style-type: none"> <li>• Link-state tracking managed interfaces can be configured with Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDU) Filtering or Mac Security Intrusion Detection.</li> <li>• The port can be enabled or disabled administratively, similar to the interface administrative status feature.</li> <li>• The port is enabled only if it is enabled in both LST and BPDU-Filtering or Mac Security. If one of them is disabled, the port is not operational and does not link up.</li> </ul>
SLPP-Guard	<ul style="list-style-type: none"> <li>• Link-state tracking managed interfaces can be configured with Simple Loop Prevention Protocol (SLPP) Guard.</li> <li>• When link-state tracking disables a port that is already disabled by SLPP-Guard, the interface is unblocked by SLPP-Guard and the blocking timer is cleared. The <code>show slpp-guard</code> command displays the details.</li> </ul>
VLACP	If enabled on interfaces, VLACP displays the upstream interface link status.
MLT	Multi-link trunks are valid members of tracking groups. However, a disabled trunk cannot be added or disabled when it is a member of a tracking group. This could allow the trunk to change its member list and can lead to various inconsistencies.
LACP – LAGs as link-state tracking members	<ul style="list-style-type: none"> <li>• LAG interfaces can be added to link-state tracking by specifying their trunk ID.</li> <li>• If several LAGs de-aggregate, during re-aggregation they can get different IDs. For example, after switch or stack reset or after each stack composition change, the LAGs are not saved into binary or ASCII configurations and are removed from tracking groups whenever de-aggregation occurs. Also, when in downstream, LAG ports must be shut down according to their LACP operational key, which is not directly under user control. An administrative key to a trunk ID can be used to ensure LAGs are persistent and maintained in LST binary or ASCII configurations and to shut down the downstream LAG member ports.</li> </ul>

*Table continues...*

Feature	Interaction
	<ul style="list-style-type: none"> <li>Until the enhancement is implemented, you cannot add LAGs to link-state tracking groups.</li> </ul>
LACP	You cannot add ports with link-aggregation enabled or enable link-aggregation on ports which are already in a tracking group.
Stack	<ul style="list-style-type: none"> <li>When entering stack, the base unit sends the LST configuration to all units. The non-base units erase their own configuration and assume the base unit configuration.</li> <li>When leaving the stack, the units keep a local version of LST configuration containing all trunks but only local ports.</li> <li>When a unit becomes inactive in stack, the local ports remain in a back-up configuration and become visible if the unit rejoins or are replaced. Adding or removing interfaces erases all back-up configuration. If a unit is replaced in stack by another unit with fewer ports, the extra ports are removed from LST configuration.</li> </ul>

### Link-state tracking configuration guidelines

The following are the guidelines to avoid configuration problems:

- You can configure up to two link-state groups per switch.
- You can configure up to eight upstream members and 384 downstream members.
- An interface cannot be a member of more than one link-state group.
- A trunk-member port cannot be added to a link-state tracking group by itself.
- Only enabled trunks can be tracking group members. A trunk which is a tracking group member cannot be disabled. If you disable and change the membership, the system displays an error 6 message.
- Ports with link aggregation enabled cannot be added to a tracking group member port.
- Operational state for interfaces or tracking groups is not saved in binary or ASCII configuration; they are dynamically determined during switch operation.

---

## Ping enhancement

Using CLI, you can specify ping parameters, including the number of Internet Control Message Protocol (ICMP) packets to be sent, the packet size, the interval between packets, and the time-out. You can also set ping to continuous, or you can set a debug flag to obtain extra debug information.

You can specify any source IPv4 address for the outgoing ICMP requests if the source address is one of the router's active layer 3 interfaces. This feature is useful for testing all routing functionality between two routers from a single place.

For more information about the ping command, see [Using the ping command to test communication with another switch](#) on page 186.



---

## New Unit Quick Configuration

Use the New Unit Quick Configuration feature to create a default configuration to apply to any new unit entering a stack configuration. You can add new units to the stack without resetting the stack.

For more information about New Unit Quick Configuration, see [Installing Ethernet Routing Switch 5900 Series](#).

---

## Updating Switch Software

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

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

- The switch has a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is on the network that is accessible by the switch and that has the desired software version loaded.
- If you change the switch software on a switch using a USB Mass Storage Device, ensure that the Mass Storage Device has the desired software version and is inserted into the front panel USB port.
- If you use CLI, ensure that CLI is in Privileged EXEC mode.
- If you use EDM, ensure that Simple Network Management Protocol (SNMP) is enabled.

### Important:

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

## LED Activity during Software Download

During the software download, the port LEDs light one after another in a chasing pattern, except for ports 35, 36, 47, and 48 on an ERS 5952GTS.

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.

For more information, see [Installing Ethernet Routing Switch 4900 Series](#) and [Installing Ethernet Routing Switch 5900 Series](#).

## Agent and diagnostic software status display

You can display the currently-loaded and operational switch or stack software status for both agent and diagnostic loads. With the `show boot` CLI command and variables, you can view the agent or

diagnostic load status individually, or together. The Boot Image EDM tab displays agent and diagnostic load status information together.

## Software download progress on EDM

EDM displays the following status messages while downloading a software:

- Software download progress percentage to indicate the time taken to download the software to the switch.
- Transferring download progress percentage to indicate the time taken to transfer the software to stack units.
- Programming percentage to indicate the time taken to write the software on the switch.
- If you are downloading software using the `NoReset` option, the Status field is updated to "success" after software download.
- Estimated remaining time until the EDM interface is operational again after switch restart. The EDM interface tries to reconnect to the switch after the estimated time has elapsed. If it is not able to reconnect immediately, the estimated reattempt time is displayed. For example, the time to reattempt to connect the to the switch can be 30 seconds.

---

## Asset ID string configuration

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

---

## Energy Saver

You can use Extreme Networks Energy Saver to reduce network infrastructure power consumption without impacting network connectivity. Energy Saver uses intelligent-switching capacity reduction in off-peak mode to reduce direct power consumption by up to 40%. Energy Saver 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 Energy Saver enabled and by the power consumption of PoE ports that are powered off. If Energy Saver for a port is set to Disabled, the port is not powered off, irrespective of the PoE configuration. Energy Saver turns off the power to a port only when PoE is enabled globally, the port Energy Saver is enabled, and the PoE priority for the port is configured to Low.

You can schedule Energy Saver to enter lower power states during multiple specific time periods. These time periods (a maximum of 84) can be as short as one minute, or last a complete week, complete weekend, or individual days.

**! Important:**

If a switch is reset while Energy Saver is activated, the PoE power-saving calculation might not accurately reflect the power saving, and in some cases might display zero savings. This problem occurs 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 is correctly updated.

When Energy Saver is active and you replace a unit, that unit will not be in Energy Saver mode. At the next deactivate/activate cycle, the unit will be in the correct state. You can issue the Energy Saver deactivate and activate command directly after replacing a unit to place the unit into the appropriate energy-savings mode.

**Table 8: Energy savings for ERS 5900**

Switch model	Typical power consumption in Normal Mode (in watts)	Typical power consumption in Energy Saver (in watts)	Savings per switch (in watts)	Savings per port (in watts)
ERS 5928GTS	77	74	3	0.125
ERS 5928GTS-PWR+ <sup>1</sup>	62	58	4	0.167
ERS 5952GTS	90	83	7	0.146
ERS 5952GTS-PWR+ <sup>1</sup>	75	69	6	0.115
ERS 5928GTS-uPWR <sup>1</sup>	67	64	3	0.125
ERS 59100GTS	187	171	16	0.167
ERS 59100GTS-PWR+ <sup>1</sup>	157	142	15	0.156
AC in = 220V, 50Hz, 2PSU, 2FAN tray				
<sup>1</sup> The power consumption values in this table can vary by up to 10%. Power consumption values can differ if a switch operates at different voltages. Power supplies operating at higher voltages are generally more efficient.				

**Table 9: Energy savings for ERS 4900**

Switch model	Typical power consumption in Normal Mode (in watts)	Typical power consumption in Energy Saver (in watts)	Savings per switch (in watts)	Savings per port (in watts)
ERS 4926GTS	44	41	3	0.125
ERS 4926GTS-PWR+ <sup>1</sup>	71	67	4	0.167
ERS 4950GTS	56	50	6	0.125

*Table continues...*

Switch model	Typical power consumption in Normal Mode (in watts)	Typical power consumption in Energy Saver (in watts)	Savings per switch (in watts)	Savings per port (in watts)
ERS 4950GTS-PWR+ <sup>1</sup>	84	77	7	0.135
AC in= 220V, 50Hz, 2PSU				
<sup>1</sup> The power consumption values in this table can vary by up to 10%. Power consumption values can differ if a switch operates at different voltages. Power supplies operating at higher voltages are generally more efficient.				

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

With this feature, you can securely transfer a 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.

The switch supports the following SFTP features:

- A binary configuration file upload to an SFTP server
- A binary configuration file download from an SFTP server
- ASCII configuration file upload to an SFTP server
- ASCII configuration file download from an SFTP server
- DSA-key authentication support
- RSA-key authentication support
- Password authentication support
- Host key generation support
- 1024-bit DSA-key use for authentication
- 1024–2048-bit RSA-key use for authentication
- Agent and diagnostic software download from an SFTP server
- SNMP and EDM support

## SFTP Server

The SFTP Server on the switch provides a volatile storage space for users to upload and download software images, licenses, configuration files, and digital certificates. Software and firmware management, configuration management, Softlic, and certificate management can access the storage space to load or export files.

To access the storage space, connect to the SSH server and request an SFTP session. The SFTP session times out when the inactive time configured in the `telnet-access-inactive-timeout` command is reached.

Read-only users can read directories, files, and file information. However, only users with read-write all access permissions can create a directory or can delete, rename, or open a file for writing.

## Limitations

This section describes the limitations associated with SFTP Server:

- Ramdisk capacity is limited to 30MB (31457280 bytes). The switch returns the error message `% Error reading image file` if there is no image file in ramdisk or if the image file is in use.
- SSH Server must be enabled.
- WinSCP and OpenSSH are recommended SFTP clients.

---

## EDM inactivity time-out

A session becomes inactive if there is no interaction with the EDM interface for more than the 15 minutes. After the session becomes inactive, you must log in again with your user name and password.

Using the CLI command `edm inactivity-timeout`, you can configure the time period for which an EDM session remains active. After the specified time period, the EDM session becomes inactive. The EDM inactivity time-out period configuration does not affect the open EDM sessions. The configuration is applied only on the future EDM sessions. By default, an EDM session becomes inactive after 15 minutes. You can configure inactivity time-out with a value between 30 and 65535 seconds.

---

## Custom logon banner

You can configure the banner that is presented when a user logs on through CLI or EDM 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.

For more information, see the following sections:

- [Customizing the CLI logon banner](#) on page 123
- [Customizing the EDM logon banner](#) on page 243

---

## Run Scripts

You can use scripts to configure the parameters for an Extreme Networks stackable Ethernet switch.

The script executes a set of CLI commands in either a fully automated or user-prompted configuration. In a fully-automated or non-verbose mode, the scripts are executed with the

predefined default values. In a user-prompted or the verbose mode, the script guides you to configure the values.

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

The run scripts delete the VLANs with the name Voice or Data, the specified IDs 42 or 44, or the IDs specified in the verbose mode, and the default routes that were applied during the previous script execution or settings applied on the switch.

**\* Note:**

Currently, only IPv4 configuration is supported.

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

Run scripts are available in both verbose and non-verbose mode for IP Office, and only verbose mode is available for Link Layer Discovery Protocol (LLDP), Auto Detect Auto Configuration (ADAC) and Shortest Path Bridging MAC (SPBM).

For more information about SPBM run script, see [Configuring Fabric Connect on Ethernet Routing Switch 4900 and 5900 Series](#).

## Run IP Office Script

The Run IP Office script can be used to configure parameters for the switch. You can execute the script in any of the following two modes using CLI or EDM:

- Non-verbose mode—configures the switch using predetermined parameters
- Verbose mode—configures the switch using the parameters provided through CLI prompts

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

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

**\* Note:**

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

**Table 10: Default parameters for Run IP Office script**

Voice VLAN ID	42
Voice VLAN 42 gateway IP	192.168.42.254

*Table continues...*

Voice VLAN Gateway IP/mask	255.255.255.0
Data VLAN ID	44
Data VLAN 44 gateway IP	192.168.44.254
Data VLAN Gateway IP/mask	255.255.255.0
IP Route to Gateway Modem-Router (Internet/WAN)	192.168.44.2
IP Office Call server address	192.168.42.1
IP Office File server address	192.168.42.1
Switch port 1 (or base_unit/1)	IP Office
Switch port 2 (or base_unit/2)	Gateway Modem-Router port

## Run ADAC script

The Run Auto Detect Auto Configuration (ADAC) script optimizes the switch configuration for IP Telephony and Unified Communications solutions to support any number of users. The Run ADAC script reduces the time required to set up the best-practice configuration of the switching parameters in a setup where:

- ADAC is used for detection and provisioning of IP Phones connected to an Ethernet switch or stack.
- LLDP is used for all configurations for voice communications over the data network.

Use the Run ADAC script to detect IP Phones using ADAC call server communication. LLDP-based detection is also possible using the Run ADAC script. ADAC is able to detect IP Phones using MAC address range detection; ADAC can also configure IP Phones as long as the IP Phones send LLDPDUs.

The ADAC script prompts the user for the Uplink, Call-Server and Telephony ports. Some of the VLAN tagging settings, LLDP network policy parameters for voice, or QoS rules are configured in the background by ADAC.

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

- Configuring VLAN ID information (for Voice and Data VLANs).
- Setting the DSCP values for Voice data and control plane (signaling).
- Applying VLAN tagging modes on switch ports to specific values for accommodating tagged (IP Phone) and untagged VLAN (laptop or desktop computer) behind the IP Phone.
- Setting call server and file server IP address to provision on the IP Phone.
- Setting ADAC Uplink, Call-Server and Telephony ports and enabling ADAC in Tagged-Frames operating mode.

## Run LLDP Script

The Run LLDP script optimizes the switch configuration for IP Telephony and Unified Communications solutions to support any number of users. The Run LLDP script reduces the time required to set up the best practice configuration of the switching parameters in a setup where LLDP is used for detection and provisioning of IP Phones connected to an Ethernet switch or stack.

Use the Run LLDP script to optimize the switch configuration for a specific deployment that does not use ADAC. ADAC-based detection is not enabled using the Run LLDP script.

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

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

## Factory default configuration

When you initially access a newly installed switch or you reset a switch to factory defaults, the switch is in a factory default configuration. This factory default configuration is the base configuration from which you build the switch configuration.

[Table 11: Factory default configuration settings](#) on page 64 outlines the factory default configuration settings present in a switch in a factory default state.

**Table 11: Factory default configuration settings**

Setting	Factory default configuration value
Unit Select switch	non-Base
Unit	1
BootP Request Mode	BootP, DHCP or Default IP mode
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

*Table continues...*



Setting	Factory default configuration value
Aging Time	300 seconds
MAC Address Security	Disabled
MAC Address Security SNMP-Locked	Disabled
Partition Port on Intrusion Detected	Disabled
Partition Time	0 seconds (the value 0 indicates forever)
DA Filtering on Intrusion Detected	Disabled
Generate SNMP Trap on Intrusion	Disabled
Clear by Ports	NONE
Learn by Ports	NONE
Trunk	blank field
Security	Disabled
Port List	blank field
Allowed Source	- (blank field)
VLAN Name	VLAN #
Management VLAN	Yes (VLAN #1)
VLAN Type	Port-based
Protocol ID (PID)	None
User-Defined PID	0x0000
VLAN State	Active (VLAN #1)
Port Membership	All ports assigned as members of VLAN 1
Filter Untagged Frames	No
Filter Unregistered Frames	Yes
Port Name	Unit 1, Port 1
PVID	1
Port Priority	0
Tagging	Untag All
AutoPVID	Enabled
Status	Enabled (for all ports)
Linktrap	On
Autonegotiation	Enabled (for all ports)
Speed/Duplex	(Refer to Autonegotiation)
Trunk Members (Unit/Port)	Blank field
STP Learning	Normal
Trunk Mode	Basic
Trunk Status	Disabled

*Table continues...*

Setting	Factory default configuration value
Trunk Name	Trunk #1 to Trunk #32
Traffic Type	Rx and Tx
Monitoring Mode	Disabled
Rate Limit Packet Type	Both
Limit	None
Snooping	Disabled
Proxy	Disabled
Robust Value	2
Query Time	125 seconds
Set Router Ports	Version 1
Static Router Ports	- (for all ports)
Console Port Speed	9600 baud
Console Switch Password	None
Telnet/Web Stack Password	None
Console Read-Only Switch Password	user
Console Read/Write Switch Password	Passwords are user/secure for non-SSH SW images and userpasswd/securepasswd for SSH SW images.
Console Read-Only Stack Password	user
Console Read/Write Stack Password	secure
Radius password/server	secret
New Unit Number	Current stack order
Group	1
Bridge Priority	8000
Bridge Hello Time	2 seconds
Bridge Maximum Age Time	20 seconds
Bridge Forward Delay	15 seconds
Add VLAN Membership	1
Tagged BPDU on tagged port	STP Group 1--No Other STP Groups--Yes
STP Group State	STP Group 1--Active Other STP Groups--Inactive
VID used for tagged BPDU	4001-4008 for STGs 1-8, respectively
STP Group	1
Participation	Normal Learning
Priority	128
Path Cost	1

*Table continues...*

Setting	Factory default configuration value
TELNET Access/SNMP/Web	By default, SNMP access is disabled in the SSH image and enabled in the non-SSH image. Telnet and Web are enabled by default in both SSH and non-SSH images. Use list: Yes
Login Timeout	1 minute
Login Retries	3
Inactivity Timeout	15 minutes
Event Logging	All
Allowed Source IP Address (50 user-configurable fields)	Entry 51: ::/0 Entry 52: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 Entry 53: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 ..... ..... Entry 100: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
	Remaining 49 fields: 255.255.255.255 (any address is allowed)
Allowed Source Mask(50 user- configurable fields)	First field: 0.0.0.0 (no IP address assigned)
	Remaining 49 fields: 255.255.255.255 (any address is allowed)
Image Filename	Zero-length string
Diagnostics image filename	Zero-length string
TFTP Server IP Address	0.0.0.0 (no IP address assigned)
Start TFTP Load of New Image	No
Configuration Image Filename	Zero-length string
Copy Configuration Image to Server	No
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
PoE admin status	Enabled
PoE Current status	Detecting
PoE Limit	16W (PWR units)/32W (PWR+ units)
PoE Port Priority	Low
PoE pd-detect-type	802dot2af_and_legacy (PWR) / 802dot3at_and_legacy (PWR+)

*Table continues...*

Setting	Factory default configuration value
PoE Power Usage Threshold	80%
PoE Traps Control Status	Enable

---

## Configuring System using CLI

The following sections provide procedures to configure the switch or stack using the Command Line Interface (CLI).

---

## Configuring Feature licenses using CLI

This section provides the procedures to install software licenses for the following features:

- Open Shortest Path First (OSPF)
- Virtual Router Redundancy Protocol (VRRP)
- Equal Cost Multi Path (ECMP)
- Protocol Independent Multicast-Sparse mode (PIM-SM)
- IPv6 Forwarding
- IP Shortcuts
- Routing Information Protocol next generation (RIPng)
- MACSec

 **Note:**

You require either an Advanced License or a Trial License to enable these features.

## Install a License File

Use the following procedure to install a license file on the switch to enable licensed features.

If the switch is reset to default, the license file must be reinstalled to reenable licensed features. Resetting a switch to default removes the license file from its storage area in NVRAM. Store the license file on a TFTP server accessible by the switch or stack before starting the installation procedure. For switches equipped with a USB port, you can also use a USB mass storage device to copy the license file to the switch.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Enter the following command:

```
copy [tftp | usb] license <tftp_ip_address> filename
<license_file_name>
```

- Restart the switch.

### Example

```
Switch>enable
Switch#copy usb license filename 5900.xml
License successfully downloaded
```

## Install a license file using SFTP

### Before you begin

- Store the license file on an SFTP server accessible by the switch or stack before starting the installation procedure.
- For authentication using an RSA or Digital Signature Algorithm (DSA) key, the authentication key must be generated and uploaded to the SFTP server.

### About this task

Follow this procedure to install a license file using SFTP.

### Procedure

- Enter Privileged EXEC mode:

```
enable
```

- Use the following command to download and install the license file if you use an RSA or DSA key for authentication.

```
copy sftp license address <sftp_ip_address> filename
<license_file_name> username <user_name>
```

- Use the following command to download and install the license file if you use a password for authentication.

```
copy sftp license address <sftp_ip_address> filename
<license_file_name> username <user_name> password
```

- Restart the switch.

### Variable definitions

Use the definitions in the following table to use the `copy sftp license` command.

Variable	Definition
<sftp_ip_address>	Specifies the address of the SFTP server.
<license_file_name>	Specifies the license file name.
<user_name>	Specifies the user name.

## Display Licenses

### About this task

Follow this procedure to display installed license files

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. Enter the following command.  
`show license`

## Delete a License

### About this task

Follow this procedure to delete an installed license.

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. Enter the following command.  
`clear license`

## Transfer a License

The switch implements Licensing Auto Unit Replacement. If a base unit fails, the other units in the stack transfer a virtual key to the new base unit to eliminate the need for transfer of a license to the new base unit. Even with this functionality in place, there are still several situations where it becomes necessary to transfer the license from one device to another. These conditions are as follows:

- Replacement of failed non-base unit.
- Incorrect MAC address entered during license file generation.
- The system displays an error message indicating the limit of MAC swaps for the license has been exceeded.

### About this task

Use the following procedure to transfer a license.

### Procedure

1. Use a web browser to access the licensing portal.
2. Enter the contact information in the required boxes.  
It is mandatory to enter an e-mail address.
3. Select **Replace or Swap a MAC address in an existing license file**.
4. Enter the License Authorization Code.
5. **(Optional)** Specify the License Bank name.
6. **(Optional)** Specify the License file name.

You can rename a license file name before it is installed on a switch.

7. Click **Submit Request**.

If you exceed the MAC replacement threshold, a message appears confirming that the MAC swap is unsuccessful. Select a different LAC entry and try again. If no other LAC entries appear in the list, contact technical support.

8. After the system displays “`MAC swap successful`”, click **Return to License Bank Details**.

9. Select the transaction that contains the license file name with the new MAC address.

10. Click **Download**.

## Base unit failure in a stack

Use only one MAC address for the license, regardless of number of units in a stack. The MAC address must be that of the base unit in the stack. After loading the license, reboot the stack. During the stack initialization process, the license functionality is enabled on every switch in the stack. If Base Unit fails, all units in the stack continue to function with the licensed features.

---

## Setting User Access Limitations

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

Ensure that you enter Global Configuration mode in CLI before you start these tasks.

### Set the Read-Only and Read/Write Passwords

To require password authentication when a user logs in to a switch, you must edit the password configuration.

#### About this task

Follow this procedure to edit the password configuration.

#### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command:

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

3. Press `Enter`.

#### Variable definitions

The following table describes the parameters for the `cli password` command.

Variable	Definition
{read-only   read-write}	Specify whether the password change is for read-only access or read-write access.
<password>	Specify password length. If password security is disabled, the password length can be 1 to 15 characters. If password security is enabled, the range for the password length is 10 to 15 characters.

## Enable and Disable Passwords

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

### About this task

Follow this procedure to enable or disable a password for a specific access method.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command:

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

3. Press **Enter**.

### Variable definitions

The following table describes the variables for the `cli password` command.

Variable	Definition
{telnet   serial}	Specify whether the password is enabled or disabled for telnet or the console. Telnet and web access are connected so that enabling or disabling passwords for one enables or disables passwords for the other.
none   local   radius   tacacs	Specify the password type to modify: <ul style="list-style-type: none"> <li>• none: disables the password.</li> <li>• local: uses the locally defined password for serial console or telnet access.</li> <li>• radius: uses RADIUS authentication for serial console or telnet access.</li> <li>• tacacs: uses TACACS+ authentication, authorization and accounting (AAA) services for serial console or telnet access.</li> </ul>



## Configure RADIUS Authentication

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

If you select RADIUS Authentication when you set up passwords through CLI, you must specify the RADIUS server settings to complete the process.

### About this task

Use this procedure to enable RADIUS authentication through CLI,

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command to configure the server settings:

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

3. From the command prompt, enter the following command to enable Change Radius Password:



```
radius-server encapsulation <MS-CHAP-V2>
```

### Variable Definitions

Use the data in the following table to use the **radius-server** command.

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

*Table continues...*

Parameter	Description
encapsulation <MS-CHAP-V2>	<p>Enables Microsoft Challenge-Handshake Authentication Protocol version 2 (MS-CHAP-V2). MSCHAP-V2 provides an authenticator controlled password change mechanism also known as the change RADIUS password function.</p> <p>DEFAULT: disabled</p> <p> <b>Note:</b> Change RADIUS Password is available only in secure software builds.</p> <p> <b>Note:</b> When you disable MS-CHAP-V2, RADIUS encapsulation is set to password authentication protocol (PAP) by default. PAP is not considered a secure encapsulation.</p>

### Related RADIUS Commands

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

1. `show radius-server`

The command has no parameters and displays the current RADIUS server configuration.

2. `no radius-server`

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

3. `radius-server password fallback`

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

---

## Configuring Run Script

Use the procedures in this section to configure IP Office, LLDP, and ADAC Run scripts.

### Configure IP Office Script

#### About this task

IP Office script automatically configures or modifies the VLAN IDs and port memberships, VLAN IP addresses, default route, QoS, and LLDP settings.

 **Note:**

Extreme Networks recommends that you execute the CLI command `run ipoffice` on a switch operating in a factory default state.

## Procedure

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

```
run ipoffice [verbose]
```

## Example

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

```
Switch>enable
Switch#run ipoffice

% The Voice VLAN ID has been set to 2
% The Voice VLAN Gateway IP address has been set to 192.0.2.24
% The Voice VLAN Gateway IP network mask has been set to 255.255.255.0
% The Data VLAN ID has been set to 3
% The Data VLAN IP address has been set to 192.0.3.24
% The Data VLAN IP network mask has been set to 255.255.255.0
%
-----
% IP Office LAN port is set to plug into switch port 1
% Gateway Modem-Router port is set to plug into switch port 2
%
-----
% Default IP Route set to 192.0.2.2 (Gateway Modem-Router interface)
% IP Office Call-Server IP address is set to 192.0.2.4
% IP Office File-Server IP address is set to 192.0.2.4
% ** Switch QoS and Unified Communications policies setup and saved **
% ** IP Office solution automated switch setup complete and saved **
%
-----
% To manage this Extreme switch, enter 192.0.0.24 in your Web browser.
%
-----
```

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

```
Switch# run ipoffice verbose

*****
*** This script will guide you through configuring the ***
*** Extreme switch for optimal operation with IP Office. ***
*** -----***
*** The values in [] are the default values, you can ***
*** input alternative values at any of the prompts. ***
*** Warning: This script may delete previous settings. ***
*** If you wish to terminate or exit this script ***
*** enter ^C <control-C> at any prompt. ***
*****
Voice VLAN ID [2] :
Voice VLAN Gateway IP Address [192.0.2.24] :203.0.113.2
Voice VLAN Gateway IP Mask [255.255.255.0] :
Data VLAN ID [3] :
Data VLAN Gateway IP Address [198.51.100.24] :203.0.133.24
Data VLAN Gateway IP Mask [255.255.255.0] :
IP Route to Gateway Modem-Router (Internet/WAN) [198.51.100.24] :203.0.113.15
IP Office Call-Server IP address [192.0.2.4] :203.0.113.20
IP Office File-Server IP address [192.0.2.4] :203.0.113.20
% The Voice VLAN ID has been set to 2
% The Voice VLAN Gateway IP address has been set to 203.0.113.2
% The Voice VLAN Gateway IP network mask has been set to 255.255.255.0
% The Data VLAN ID has been set to 3
% The Data VLAN IP address has been set to 203.0.113.24
% The Data VLAN IP network mask has been set to 255.255.255.0
%
-----
% IP Office LAN port is set to plug into switch port 1
```

```

% Gateway Modem-Router port is set to plug into switch port 2
%
-----
% Default IP Route set to 203.0.113.15 (Gateway Modem-Router interface)
% IP Office Call-Server IP address is set to 203.0.113.20
% IP Office File-Server IP address is set to 203.0.113.20
% ** Switch QoS and Unified Communications policies setup and saved **
% ** IP Office solution automated switch setup complete and saved **
%
-----
% To manage this Extreme switch, enter 203.0.133.24 in your Web browser.
%
-----

```

**\* Note:**

If there is an error, the script execution stops and the system displays an error message.

## Configure ADAC Script using CLI

### About this task

Run ADAC script detects IP Phones using ADAC call server communication. Also, the script detects all the configurations for voice communications over the data network using LLDP.

The ADAC script prompts for the Uplink, Call-Server and Telephony ports. Some of the VLAN tagging settings, LLDP network policy parameters for voice, or QoS rules are configured in the background by ADAC.

**\* Note:**

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

### Procedure

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

```
run adac
```
3. Enter the information requested at each prompt.

### Example

The following is the sample output for `run adac` command script.

```

Switch# run adac
*****
*** This script will guide you through configuring the ***
*** Extreme switch for optimal operation using ADAC. ***
*** -----***
*** Input required values at each prompts. ***
*** If you wish to terminate or exit this script ***
*** enter ^C <control-C> at any prompt. ***
*** Warning: This script may delete previous settings. ***
*****
Data VLAN ID [2-4094 or Enter to skip]:
Do you want to use the Data VLAN as the management VLAN [yes/no]?
Default IP Route [A.B.C.D]:
Data VLAN Gateway IP address [A.B.C.D or Enter to skip]:
Data VLAN Gateway IP netmask [xxx.xxx.xxx.xxx/xx]:
Management IP address [A.B.C.D or Enter to skip]:
Management IP netmask [xxx.xxx.xxx.xxx or Enter to skip]:
Voice VLAN ID [2-4094]:

```

```

Voice VLAN Gateway IP address [A.B.C.D or Enter to skip]:
Voice VLAN Gateway IP netmask [xxx.xxx.xxx.xxx/xx]:
LLDP Call-Server IP address [A.B.C.D]:
LLDP File-Server IP address [A.B.C.D]:
Do you want to configure a MLT Trunk as Uplink port? [yes/no]
Uplink Trunk port members [slot/port,slot/port...]:
ADAC Uplink ports [slot/port,slot/port...]:
ADAC Call Server ports [slot/port,slot/port...]:
ADAC Telephony ports [slot/port,slot/port...]:
% The Data VLAN ID is set to [according to the provided input]
% The Data VLAN [according to the provided input] is set as Management VLAN
% The Default IP Route is set to [according to the provided input]
% The Data VLAN Gateway IP address is set to [according to the provided input]
% The Data VLAN Gateway IP netmask is set to [according to the provided input]
% The Management IP address is set to [according to the provided input]
% The Management IP netmask is set to [according to the provided input]
% The Voice VLAN ID is set to [according to the provided input]
% The Voice VLAN Gateway IP address is set to [according to the provided input]
% The Voice VLAN Gateway IP netmask is set to [according to the provided input]
% LLDP Call Server IP address is set to [according to the provided input]
% LLDP File Server IP address is set to [according to the provided input]
% The ADAC Uplink ports are set to [according to the provided input]
% The ADAC Call Server ports are set to [according to the provided input]
% The ADAC Telephony ports are set to [according to the provided input]
% ** ADAC operating mode is set to tagged frames **
% ** ADAC is now enabled **
% ** Switch QoS and Unified Communications policies setup and saved **
% -----
% To manage this Extreme switch, enter [MGMT VLAN IP entry] in your Web browser.
% -----

```

## Configure LLDP Script using CLI

### About this task

Configures or modifies the LLDP and Voice VLAN using VLAN ID, IP addresses, LLDP MED policies, and QoS rules.

### Procedure

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

```
run lldp
```
3. Enter the information requested at each prompt.

### Example

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

```

*****
*** This script will guide you through configuring the ***
*** Extreme switch for optimal operation using LLDP. ***
*** -----***
*** Input required values at each prompts. ***
*** If you wish to terminate or exit this script ***
*** enter ^C <control-C> at any prompt. ***
*** Warning: This script may delete previous settings. ***
*****
Data VLAN ID [2-4094 or Enter to skip]:

```

## System Configuration

```
Do you want to use the Data VLAN as the management VLAN [yes/no]?
Default IP Route [A.B.C.D]:
Data VLAN Gateway IP address [A.B.C.D or Enter to skip]:
Data VLAN Gateway IP netmask [xxx.xxx.xxx.xxx/xx]:
Data VLAN Uplink ports [unit/port, unit/port..]:
Management IP address [A.B.C.D or Enter to skip]:
Management IP netmask [xxx.xxx.xxx.xxx/xx]:
Voice VLAN ID [2-4094]:
Voice VLAN Gateway IP address [A.B.C.D or Enter to skip]:
Voice VLAN Gateway IP netmask [xxx.xxx.xxx.xxx/xx]:
LLDP Call-Server IP address [A.B.C.D]:
LLDP File-Server IP address [A.B.C.D]:
% The Data VLAN ID is set to [according to the provided input]
% The Data VLAN [according to the provided input] is set as Management VLAN
% The Default IP Route is set to [according to the provided input]
% The Data VLAN Gateway IP address is set to [according to the provided input]
% The Data VLAN Gateway IP netmask is set to [according to the provided input]
% The Data VLAN Uplink ports [according to the provided input] tagging is set to tagAll
% The Management IP address is set to [according to the provided input]
% The Management IP netmask is set to [according to the provided input]
% The Voice VLAN ID is set to [according to the provided input]
% The Voice VLAN Gateway IP address is set to [according to the provided input]
% The Voice VLAN Gateway IP netmask is set to [according to the provided input]
% LLDP Call Server IP address is set to [according to the provided input]
% LLDP File Server IP address is set to [according to the provided input]
% ** Switch QoS and Unified Communications policies setup and saved **
% -----
% To manage this Extreme switch, enter [MGMT VLAN IP entry] in your Web browser.
% -----
```

---

## Change Switch Software

### ! Important:

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

### About this task

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

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

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

During the download, the switch is not operational.

You can track the progress of the download by observing the front panel LEDs. For more information about this topic, see [LED Activity during Software Download](#) on page 57.

## Procedure

1. Access CLI through the telnet protocol or through a console connection.
2. At the command prompt, enter the following command:

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

3. Press Enter.

## Variable definitions

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

Variable	Definition
sftp	Download from the SFTP server.
address <A.B.C.D>   <WORD>	The IPv6 or IP address of the TFTP or SFTP server you use. The address <A.B.C.D>   <WORD> parameter is optional and if you omit it, the switch defaults to the TFTP or SFTP server specified by the <code>tftp-server</code> or <code>sftp-server</code> command unless software download is to occur using a USB Mass Storage Device.
image <image name>	The name of the software image to be downloaded from the TFTP or SFTP server.
image-if-newer <image name>	This parameter is the name of the software image to be downloaded from the TFTP server if it is newer than the currently running image.
diag <image name>	The name of the diagnostic image to be downloaded from the TFTP or SFTP server.
poe_module_image <image name>	The name of the Power over Ethernet module image to be downloaded from the TFTP server. This option is available only for switches that support Power Over Ethernet.
no-reset	This parameter forces the switch to not reset after the software download is complete.
usb	Specifies that the software download is performed using a USB Mass Storage Device and the front panel USB port.
primary	Download the primary agent image from the TFTP or SFTP server.
secondary	Download the secondary agent image from the TFTP or SFTP server.
The <code>image</code> , <code>image-if-newer</code> , <code>diag</code> , and <code>poe_module_image</code> parameters are mutually exclusive; you can execute only one at a time.	
The <code>address &lt;ip&gt;</code> and <code>usb</code> parameters are mutually exclusive; you can execute only one at a time.	

---

## Toggle the Dual Agent next Boot Image

Use this procedure to toggle the next boot image.

## About this task

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

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

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

## Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

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

```
toggle-next-boot-image
```

### \* Note:

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

---

## Setting TFTP Parameters

Many processes in the switch can use a Trivial File Transfer Protocol (TFTP) server. You can set a default TFTP server for the switch and clear these defaults through CLI.

### ! Important:

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

## Set a Default TFTP Server

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

- Changing switch software using CLI.
- Copying running-config tftp command.
- Copying config tftp command.



**About this task**

Use this procedure to specify a default TFTP server for the switch.

**Procedure**

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
tftp-server [<A.B.C.D> | <WORD>]
```
3. Press Enter.

**Variable definitions**

Use the data in the following table to use the **tftp-server** command.

Variable	Definition
<i>A.B.C.D</i>	Specifies the IP address of TFTP server.
<i>WORD</i>	Specifies the IPv6 address of TFTP server.

**Display the TFTP Server****About this task**

Displays the default TFTP server configured for the switch.

**Procedure**

1. Enter Privileged EXEC mode:  

```
enable
```
2. Display the TFTP server configured for the switch:  

```
show tftp-server
```
3. Press Enter.

**Clear the Default TFTP Server****About this task**

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

**Procedure**

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter one of the following commands:

```
no tftp-server
```

OR

```
default tftp-server
```

3. Press Enter.

---

## Configuring SFTP using CLI

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

- Changing switch software using CLI.
- Copying running-config sftp command.
- Copying config sftp command.

Use the information in this section to configure the switch to use an SFTP server.

### Configure a Default SFTP Server IP Address using CLI

#### About this task

Use this procedure to specify a default SFTP server IP address.

#### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
sftp-server [<A.B.C.D> | <WORD>]
```

3. Press Enter.

#### Variable definitions

Use the data in the following table to use the *sftp-server* command.

Variable	Definition
<A.B.C.D>	Specify an IPv4 address for the SFTP server.
<WORD>	Specify an IPv6 address for the SFTP server.

### Clear the Default SFTP Server IP Address using CLI

#### About this task

Use this procedure to clear the SFTP server IP address and reset it to 0.0.0.0.

## Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. From the command prompt, enter the following command:  
`no sftp-server`  
OR  
`default sftp-server`
3. Press Enter.

## Display the Default SFTP Server IP Address using CLI

### About this task

Use this procedure to display the default SFTP server IP address configured for the switch.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:  
`show sftp-server`
3. Press Enter.

---

## Configuring files in CLI

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

## Display the Current Configuration

### About this task

Use this procedure to display the current configuration of switch or a stack. You can use the command with or without parameters.

#### Important:

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

**! Important:**

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

**Procedure**

1. Enter Privileged EXEC mode:

```
enable
```

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

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

**\* Note:**

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

3. Press Enter.

**Example**

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

**Table 12: show running-config module mlt command output**

```
Switch# show running-config module mlt

! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch <Switch#>
! Software version = vx.x.x.xx
!
! Displaying only parameters different to default
!=====
enable
configure terminal
!
! *** MLT (Phase 1) ***
!
!
! *** MLT (Phase 2) ***
```

**Table 13: show running-config module ip mlt command output**

```
Switch# show running-config module ip mlt

! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch <Switch#>
Software version = vx.x.x.xx
```

```

!
! Displaying only parameters different to default
!=====
enable
configure terminal
!
! *** IP ***
!
ip default-gateway 192.0.2.24
ip address switch 192.0.2.15
ip address netmask 255.255.255.0
!
! *** MLT (Phase 1) ***
!
!
! *** MLT (Phase 2) ***
!
!

```

**Table 14: show running-config command output**

```

Switch# show running-config verbose

Switch(config)#show running-config verbose
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch <Switch#>
! Software version = vx.x.x.xx
!
! Displaying all switch parameters
!=====
enable
configure terminal
!
! *** AAA ***

password aging-time 0
password password-history 3
password complexity lower-case 0
password complexity numeric 0
password complexity special 0
password complexity upper-case 0
password min-length 8
password notifications 10
password check-sequential enable
password check-repeated enable
password delay-time 60
password password-change-rate-limiter 1
password password-change-on-first-login disable
password unlock-timer 7
no password login-failure-notification
! *** CORE (Phase 1) ***

```

*Table continues...*

## System Configuration

```
!  
tftp-server 172.16.3.2  
!  
! *** SNMP ***  
!  
!  
! *** IP ***  
!  
ip default-gateway 192.0.2.24  
ip address switch 192.0.2.15  
  
!  
! *** IP Manager ***  
!  
!  
! *** ASSET ID ***  
!  
!  
! *** IPFIX ***  
!  
!  
! *** System Logging ***  
!  
!  
! *** STACK ***  
!  
!  
! *** Custom Banner ***  
!  
!  
! *** SSH ***  
!  
!  
! *** SSL ***  
!  
!  
! *** SSHC ***  
!  
!  
! *** MSTP (Phase 1) ***  
!  
!  
! *** LACP (Phase 1) ***  
  
!  
!LACP mode is set to OFF on all interfaces to enable manipulation of  
!ports with LACP enabled  
interface Ethernet ALL  
lacp mode port ALL off  
exit  
!  
! *** VLAN ***  
!
```

```
!  
! *** 802.1ab ***  
!  
interface Ethernet ALL  
lldp tx-tlv port ALL dot3 mac-phy-config-status  
exit  
!  
! *** 802.1ab vendor-specific Extreme TLVs config ***  
!  
! *** 802.1AB MED Voice Network Policies ***  
!  
! *** QOS ***  
!  
! *** RMON ***  
!  
! *** SPBM (Phase 1) ***  
!  
!spbm  
!spbm reserved-port stack  
router isis  
overload  
exit  
!  
! *** EAP ***  
!  
! *** EAP Guest VLAN ***  
!  
! *** EAP Fail Open VLAN ***  
!  
! *** EAP Voip VLAN ***  
!  
! *** Interface ***  
!  
! *** Rate-Limit ***  
!  
! *** MLT (Phase 1) ***  
!  
! *** MAC-Based Security ***  
!  
! *** LACP (Phase 2) ***
```

## System Configuration

```
!  
!  
! *** ADAC ***  
!  
!  
! *** MSTP (Phase 2) ***  
!  
!  
! *** Port Mirroring ***  
!  
!  
! *** VLAN Phase 2***  
!  
!  
! *** MLT (Phase 2) ***  
!  
!  
! *** PoE ***  
!  
!  
! *** RTC ***  
!  
! clock set 09:04:36 19 August 2017  
!  
! *** Extreme Energy Saver ***  
!  
!  
! *** AUR ***  
!  
!  
! *** AAUR ***  
!  
!  
! *** L3 ***  
!  
!  
! --- ECMP ---  
!  
! No license for ECMP.  
! Contact extremeportal.force.com/ to update Software license.  
!  
! *** Brouter Port ***  
!  
!  
! *** CORE (Phase 2) ***  
!  
!  
! *** IPV6 ***  
interface vlan 1  
ipv6 interface  
exit  
!  
! *** MLD ***
```



```
!  
interface vlan 1  
ipv6 mld  
exit  
!  
! *** FHS ***  
!  
! --- FHS Global settings ---  
!  
! --- IPV6 access list settings ---  
!  
! --- IPv6 mac access list settings ---  
!  
! --- IPV6 dhcp guard settings ---  
!  
! --- IPV6 RA Guard settings ---  
!  
! --- IPV6 Policy Port Map settings ---  
!  
! --- IPV6 FHS ND SBT Table settings ---  
!  
! --- IPV6 Source Guard Interface settings ---  
!  
! *** RIPNG ***  
!  
router rip  
router rip ipv6-enable  
ipv6 default-information enable  
exit  
interface vlan 1  
ipv6 rip enable  
ipv6 rip default-information only  
ipv6 rip poison  
exit  
!  
! *** VRRPV3 ***  
!  
! *** SPBM (Phase 2) ***  
!  
! *** VLACP ***  
!  
!
```

## System Configuration

```
! *** DHCP Relay ***
!
!
! *** L3 Source Interface ***
!
!
! *** L3 Protocols ***
!
! --- IP Directed Broadcast ---
!
! --- Proxy ARP ---
!
! --- UDP Broadcast Forwarding ---
!
! --- VRRP ---
!
! --- Route Policies ---
!
ip prefix-list "test" 1.1.1.1/0
route-map "test" 2
route-map "test" 2 enable
route-map "test" 2 match protocol direct
!
! --- OSPF ---
!
router ospf
router-id 198.51.100.0
accept adv-rtr 1.1.1.1 route-policy "test"
exit
!
! --- RIP ---
!
interface vlan 1
ip rip in-policy "test"
ip rip out-policy "test"
exit
!
! *** IP Forwarding Next-Hop ***
!
!
! *** DHCP SNOOPING ***
!
!
! *** ARP INSPECTION ***
!
!
! *** IP SOURCE GUARD ***
```

```

!
!
! *** IGMP ***
!
interface vlan 1
ip igmp snooping
ip igmp proxy
ip igmp version 3
ip igmp mrouter 4
exit
ip igmp profile 1
range 0.0.0.0
exit
!
! *** MVR ***
!
! *** STACK MONITOR ***
!
! *** SLPP-guard ***
!
! *** PIM ***
!
! *** CFM ***
!
! *** SLAMON ***
!
! *** STORM CONTROL ***
!
! *** LINK STATE TRACKING ***
!
! *** SFLOW ***
!
! *** Fabric Attach ***
!
!

```

**\* Note:**

When the software is upgraded from a release that does not support Password complexity and Password aging and lockout, some of the default values change for the feature as follows:

```

password aging-time 90
password password-history 3
password complexity lower-case 2

```

```

password complexity numeric 2
password complexity special 2
password complexity upper-case 2
password min-length 10
password notifications 30

```

## Variable definitions

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

Variable	Definition
module <value>	<p>Display configuration of an application for any of the following parameter values:</p> <p>[802.1ab] [aaa] [aaur] [adac] [arp-inspection] [asset-id] [aur] [banner] [brouter] [cfm] [core] [dhcp-relay] [dhcp-snooping] [eap] [energy-saver] [fa] [igmp] [interface] [ip ] [ip-source-guard] [ipfix] [ipmgr] [ ipv6 ] [ipv6-fhs] [l3] [l3-protocols] [lacc] [link-state] [logging] [mac-security] [mld] [mlt] [mvr] [pim] [port-mirroring] [qos] [radius] [rate-limit] [ripng] [rmon] [rtc] [sflow] [slamon] [slpp] [snmp] [spbm] [ssh] [sshc] [ssl] [stack] [stkmon] [storm-control] [stp] [tacacs] [vlacc] [vlan] [vrrpv3]</p>
verbose	Display entire configuration, including defaults and non-defaults.

## Storing the Current Configuration in ASCII File

You can store the current configuration into an ASCII file, on a TFTP server, SFTP server or USB Mass Storage Device (through the front panel USB drive).

### \* Note:

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

## Copy Current Configuration File to the TFTP Server

### About this task

Use this procedure to copy contents of the current configuration file to another file on the TFTP server.

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

### \* Note:

You can execute this command in the Privileged EXEC command mode or the Global Configuration command mode.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

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

- Press Enter.

### Variable definitions

Use the data in the following table to use the `copy running-config tftp` command.

Variable	Definition
address <A.B.C.D>   <WORD>	Specify the IP address of the TFTP server. <ul style="list-style-type: none"> <li>A.B.C.D—Specify the IP address</li> <li>WORD—Specify the IPv6 address</li> </ul>
filename <WORD>	Specify the file name to store configuration commands on the TFTP server.
module <applicationModules>	Display configuration of an application for any of the following parameter values: [802.1ab] [aaa] [aaur] [adac] [arp-inspection] [asset-id] [aur] [banner] [brouter] [cfm] [core] [dhcp-relay] [dhcp-snooping] [eap] [energy-saver] [fa] [igmp] [interface] [ip] [ip-source-guard] [ipfix] [ipmgr] [ipv6] [ipv6-fhs] [l3] [l3-protocols] [lacp] [link-state] [logging] [mac-security] [mld] [mlt] [pim] [port-mirroring] [qos] [radius] [rate-limit] [ripng] [rmon] [rtc] [slamon] [slpp] [snmp] [spbm] [ssh] [sshc] [ssl] [stack] [stkmon] [storm-control] [stp] [tacacs] [vlacp] [vlan]
verbose	Copy the entire configuration, including defaults and non-defaults.

## Copy Current Configuration file to a USB Device

### About this task

Use this procedure to copy the contents of the current configuration file to a USB storage device.

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

#### Note:

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

### Procedure

- Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

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

- Press Enter.

### Variable definitions

Use the data in the following table to use the `copy running-config usb` command.

Variable	Definition
filename <WORD>	Specify the file name to store configuration commands on the TFTP server.
module <applicationModules>	Display configuration of an application for any of the following parameter values:  [802.1ab] [aaa] [aaur] [adac] [arp-inspection] [asset-id] [aur] [banner] [brouter] [cfm] [core] [dhcp-relay] [dhcp-snooping] [eap] [energy-saver] [fa] [igmp] [interface] [ip] [ip-source-guard] [ipfix] [ipmgr] [ipv6] [ipv6-fhs] [l3] [l3-protocols] [lacp] [link-state] [logging] [mac-security] [mld] [mlt] [pim] [port-mirroring] [qos] [radius] [rate-limit] [ripng] [rmon] [rtc] [slamon] [slpp] [snmp] [spbm] [ssh] [sshc] [ssl] [stack] [stkmon] [storm-control] [stp] [tacacs] [vlacp] [vlan]
verbose	Copy the entire configuration, including defaults and non-defaults.

### Copy Current Configuration File to SFTP Server

#### About this task

Use this procedure to copy contents of the current configuration file to another file on the SFTP server.

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

#### \* Note:

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

#### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
copy running-config sftp [verbose] [module <applicationModules >]
([address {<A.B.C.D> | <WORD> }]) filename <WORD> username <WORD>
[password]
```

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `copy running-config sftp` command.

Variable	Definition
address <A.B.C.D>   <WORD>	Specify the address of the SFTP server to be used: <ul style="list-style-type: none"> <li>• A.B.C.D—specify the IPv4 address.</li> <li>• WORD—specify the IPv6 address.</li> </ul>

*Table continues...*

Variable	Definition
filename <WORD>	Specify the name of the file that is created when the configuration is saved to the TFTP or SFTP server or USB Mass Storage Device.
username <WORD>	Specify the user name.
password	If sshc password authentication is enabled, then the password parameter is mandatory.
module <applicationModules>	Display the configuration of an application for any of the following parameter values:  [802.1ab] [aaur] [adac] [arp-inspection] [asset-id] [aur] [banner] [brouter] [cfm] [core] [dhcp-relay] [dhcp-snooping] [eap] [energy-saver] [fa] [igmp] [interface] [ip] [ip-source-guard] [ipfix] [ipmgr] [ipv6] [ipv6-fhs] [l3] [l3-protocols] [lACP] [link-state] [logging] [mac-security] [mld] [mlt] [mvr] [pim] [port-mirroring] [qos] [radius] [rate-limit] [rmon] [rtc] [sflow] [slamon] [slpp] [snmp] [spbm] [ssh] [sshc] [ssl] [stack] [stkmon] [storm-control] [stp] [tacacs] [vlacp] [vlan]
verbose	Copy the entire configuration for the switch or stack (defaults and non-defaults).

## Create an Entry in the ASCII Configuration Script Table

### About this task

Use this procedure to create an entry (either a TFTP, an SFTP or a USB entry) in the ASCII configuration script table.

#### Important:

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `script` command.

Variable	Definition
<1-127>	The index of the entry to be used.
bootp	Indicate script from the TFTP server, file name, and IP address obtained using BOOTP.
load-on-boot	Specify the load-on-boot priority. Values range from 1 to 127. If you omit this parameter, the entry is created or modified for manual upload and downloads only.
filename	The name of the file to be saved.
tftp	Create a TFTP entry. Script from TFTP server.
sftp	Create an SFTP entry. Script from SFTP server.
<A.B.C.D >  <WORD>	Specify the hostname or IPv4 address, or the IPv6 address of the TFTP or SFTP server.
username <WORD>	Specify the user name.
password	Specify the password.
usb	Create a USB entry.
unit <1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack.

## View Status of Entries in ASCII Configuration Script Table

### About this task

Use this procedure to view the status of one or all the entries in the ASCII configuration script table.

### Procedure

1. Enter Privileged EXEC mode:  

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

```
show script status [<1-127>]
```
3. Press Enter.

### Variable definitions

Use the data in the following table to use the `show script status` command.

Variable	Definition
<1-127>	The index of the entry to be used.

## Storing the Current Configuration in Binary File

You can store the current configuration into binary files, on a TFTP server, SFTP server or USB Mass Storage Device (through the front panel USB drive).



## Store Configuration to TFTP Server

### About this task

Use this procedure to store configuration in the binary file to a TFTP server.

#### Important:

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

3. Press Enter.

### Variable definitions

The following table describes the variables for the `copy config tftp` command.

Variable	Description
address <A.B.C.D>   <WORD>	Specifies the IP address of the TFTP server. <ul style="list-style-type: none"> <li>• A.B.C.D—specifies the IP address</li> <li>• WORD—specifies the IPv6 address</li> </ul>
filename <filename>	The name of the file to be retrieved.

## Store Configuration to SFTP Server

### About this task

Use this procedure to store configuration in the binary file to a SFTP server.

#### Important:

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

3. Press Enter.

### Variable definitions

The following table describes the variables for the `copy config sftp` command.

Variable	Description
address <A.B.C.D>   <WORD>	Specifies the address of the SFTP server: <ul style="list-style-type: none"> <li>• A.B.C.D—specifies the IPv4 address.</li> <li>• WORD—specifies the IPv6 address.</li> </ul>
filename <filename>	Specifies the name of the configuration file on the SFTP server.
username <WORD>	Specifies the username.
password <WORD>	Specifies the password — mandatory when password authentication is enabled

## Store Configuration in a USB Device

### About this task

Use this procedure to store a configuration file to a USB Mass Storage Device.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

3. Press Enter.

### Variable definitions

The following table describes the variables for the `copy config usb` command.

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

## Restoring Configuration from an ASCII File

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

- [Restoring configuration using the configure command](#) on page 98
- [Creating an entry in the ASCII configuration script table](#) on page 99

## Restore Configuration using the Config Command

### About this task

Use this procedure to restore contents of the current configuration from an ASCII file using the `configure {network | usb | sftp}` command.

## Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

3. Press Enter.

## Variable definitions

The following table describes the variables for the `configure {network | usb | sftp}` command.

Variable	Description
network	Retrieve the configuration from a TFTP server.
usb	Retrieve the configuration from an USB mass storage device.
sftp	Retrieve the configuration from a SFTP server.
<1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack.
address <A.B.C.D>   <WORD>	Specifies the address of the SFTP server: <ul style="list-style-type: none"> <li>• A.B.C.D—specifies the IP address</li> <li>• WORD—specifies the IPv6 address</li> </ul>
filename <WORD>	The name of the file to be retrieved.
username <WORD>	Specifies the username.
password	Specifies the password.

## Create an Entry in the ASCII Configuration Script Table

### About this task

Use this procedure to create an entry (either a TFTP, a SFTP or an USB entry) in the ASCII configuration script table.

### Important:

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

## Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

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

- Press Enter.

### Variable definitions

The following table describes the variables for the `script` command.

Variable	Description
<1-127>	The index of the entry to be restored.
bootp	Indicates script from the TFTP server, filename, and IP address obtained using BOOTP.
load-on-boot	Specifies the load-on-boot priority. Values range from 1 to 127. If you omit this parameter, the entry is created or modified for manual upload and downloads only.
filename	The name of the file to be restored.
username <WORD>	Specifies the username.
tftp	Restores a TFTP entry
sftp	Restores a SFTP server.
A.B.C.D >   <WORD>	Specifies the address of the SFTP or TFTP server: <ul style="list-style-type: none"> <li>A.B.C.D—specifies the IPv4 address.</li> <li>WORD—specifies the IPv6 address.</li> </ul>
usb	Restores an USB entry.
unit <1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack.

### View Status of Entries in ASCII Configuration Script Table

#### About this task

Use this procedure to view the status of one or all the entries.

#### Note:

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

#### Procedure

- Enter Privileged EXEC mode:

```
enable
```
- At the command prompt, enter the following command:

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

3. Press Enter.

### Example

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

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

### Variable definitions

The following table describes the variables for the `show script status` command.

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

## Load the Script from an ASCII File

### About this task

Use this procedure to load the script from an ASCII file to a tftp server, sftp server, or USB Mass Storage Device.

#### Important:

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

3. Press Enter.

### Variable definitions

The following table describes the variables for the `script run` command.

Variable	Description
<1-127>	The index of the ASCII configuration script table entry to be used.
<filename>	The name of the file to be restored.
username <WORD>	Specifies the user name.

*Table continues...*

Variable	Description
unit <1-8>	The unit number in which the USB device is inserted in, if the unit is a part of the stack.
sftp	Restores a SFTP server.
tftp	Restores a TFTP server.
<A.B.C.D>   <WORD>	Specifies the address of the SFTP or TFTP server to load the script. <ul style="list-style-type: none"> <li>A.B.C.D—specifies the IPv4 address.</li> <li>WORD—specifies the IPv6 address.</li> </ul>

## Upload the Current ASCII Configuration

### About this task

Use this procedure to upload the current ASCII configuration using an entry in the ASCII configuration script table.

#### Important:

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Upload the current ASCII configuration:

```
script upload <1-127> [module] {[802.1ab] [aaa] [aur] [adac] [arp-
inspection] [asset-id] [aur] [banner] [brouter] [cfm] [core] [dhcp-
relay] [dhcp-snooping] [eap] [energy-saver] [fa] [igmp] [interface]
[ip] [ip-source-guard] [ipfix] [ipmgr] [ipv6] [ipv6-fhs] [l3] [l3-
protocols] [lACP] [link-state] [logging] [mac-security] [mld] [mlt]
[mvr] [pim] [port-mirroring] [qos] [radius] [rate-limit] [ripng]
[rmon] [rtc] [sflow] [slamon] [slpp] [snmp] [spbm] [ssh] [sshc]
[ssl] [stack] [stkmon] [storm-control] [stp] [tacacs] [vlACP]
[vlan]}
```

## Display the ASCII Configuration File Status

### About this task

Use this procedure to view the status of the ASCII configuration file.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

```
show script block
```

- Press Enter.

### Example

```
Switch(config)#show script block
```

```
-----
Block  Name                Last Used  Last Status
-----
1      script_block_1          YES        Pass
2      script_block_2          NO         Fail
```

### Variable definitions

The following table describes the fields in the `show script block` command.

Variables	Description
Block	Specifies the block assigned to the ASCII configuration file when downloaded.
Name	Specifies the name for the local ASCII configuration file. If no ASCII configuration files have been downloaded, this field remains blank.
Last Used	Indicates whether an ASCII configuration file was used the last time the system was booted.
Last Status	Indicates the status of the last execution, either Pass or Fail. If an ASCII configuration file was not used, this field displays Fail.

## Download an ASCII Configuration File from a TFTP Server or USB Device

### About this task

Use this procedure to download an ASCII configuration file from a TFTP server or USB device to the local ASCII file system. You can then boot the system from the local file system. In a stack, the downloaded ASCII configuration file will be saved in all units.

### Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- To download from a TFTP server, enter the following command at the command prompt:

```
copy tftp script address <address> filename <filename> block <1-2>
[name <name>]
```

- To download from a USB device, enter the following command at the command prompt:

```
copy usb script filename <filename> block <1-2> [name <name>]
```

### Next steps

Proceed with the `boot script` command to boot the system with the local ASCII configuration file.

Once the system boots successfully with an ASCII configuration file, the system configuration is saved to the binary configuration. If the system boot fails, the system resets and boots with the current binary configuration.

For the boot command, see [Setting boot parameters](#) on page 118.

## Variable definitions

The following table describes the fields in the `copy [tftp] [usb] script` command.

Variable	Description
address <A.B.C.D>   <WORD>	Specifies the address of the TFTP server to load the script. <ul style="list-style-type: none"> <li>A.B.C.D - specifies the IPv4 address</li> <li>WORD - specifies the IPv6 address</li> </ul>
filename <WORD>	Specifies the name of the file to be retrieved.
block <1-2> [name <WORD>]	Specifies the block from which the ASCII configuration file is to be downloaded.  If you do not specify a name for the block name, the default is the name of the file retrieved.

## Restoring Configuration from a Binary File

You can restore the configuration from a binary file.

### Note:

The IP of the management VLAN does not change after the binary configuration of the device. As a result, the VRRP configuration for the management VLAN will not be saved or retrieved from the binary configuration file.

## Restore a Configuration from a TFTP Server

### About this task

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

### Important:

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

3. Press Enter.



### Variable definitions

The following table describes the variables for the `copy tftp config` command.

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

## Restore a Configuration from a SFTP Server

### About this task

Use this procedure to restore a configuration from a binary file from a SFTP server.

#### Important:

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

3. Press Enter.

### Variable definitions

The following table describes the variables for the `copy sftp config` command.

Variable	Description
address <A.B.C.D> <WORD>	Specifies the address of the SFTP or TFTP server to load the script. <ul style="list-style-type: none"> <li>• A.B.C.D—specifies the IPv4 address.</li> <li>• WORD—specifies the IPv6 address.</li> </ul>
filename <WORD>	Specifies the name of the file to be retrieved.
username <WORD>	Specifies the username.
password	Specifies the password.

## Restore a Configuration File from a USB Mass Storage Device

### About this task

Use this procedure to restore a configuration file from a USB Mass Storage Device. The only parameter for this command is the name of the file to be retrieved from the USB device.

**Procedure**

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`copy usb config filename <name>`
3. Press Enter.

**Variable definitions**

The following table describes the variables for the `copy usb config` command.

Variable	Description
filename <filename>	Specifies the name of the file to be retrieved.

**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.

**Copy the Current Configuration to NVRAM using the Write Command****About this task**

Use this procedure to copy the current configuration to NVRAM. This command has no parameters or variables.

**Procedure**

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`write memory`
3. Press Enter.

**Copy the Current Configuration to NVRAM using the Save Command****About this task**

Use this procedure to copy the current configuration to NVRAM. This command has no parameters or variables.

**Procedure**

1. Enter Privileged EXEC mode:  
`enable`

- At the command prompt, enter the following command:

```
save config
```

- Press Enter.

## Downloading of a Configuration file (automatic)

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

### ! Important:

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

## Load a Configuration File using the Configure Command

### About this task

Use this procedure to immediately load the configure parameters to automatically download a configuration file when the switch or stack is booted.

### Procedure

- Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

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

- Enter the following command to view the current switch settings for this process:


```
show config-network
```

### Variable Definitions

The following table describes the variables for the `configure network` command.

Variable	Description
load-on-boot {disable   use-bootp   use-config}	<p>The settings to automatically load a configuration file when the system boots:</p> <ul style="list-style-type: none"> <li><b>disable:</b> disable the automatic loading of config file</li> <li><b>use-bootp:</b> load the ASCII configuration file at boot and use BootP to obtain values for the TFTP or SFTP address and file name</li> <li><b>use-config:</b> load the ASCII configuration file at boot and use the locally configured values for the TFTP or SFTP address and file name</li> </ul>

*Table continues...*

Variable	Description
	 <b>Important:</b> If you omit this parameter, the system immediately downloads and runs the ASCII configuration file.
address <A.B.C.D   WORD>	Specifies the address of the TFTP server: <ul style="list-style-type: none"> <li>• A.B.C.D—specifies the IPv4 address.</li> <li>• WORD—specifies the IPv6 address.</li> </ul>
filename <WORD>	Specifies the name of the configuration file to use in this process.

## Load a Configuration File using Script Command

### About this task

Use this procedure to run a script to automatically download a configuration file when the switch or stack is booted.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Enter the following command to view the current switch settings for this process:

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

### Variable definitions

The following table describes the variables for the `script` command.

Variable	Description
script <1-127>	The index of the ASCII configuration script table entry to be used.
load-on-boot <1-127>	The boot priority of the ASCII configuration script table entry.
[usb   tftp   sftp   bootp]	The settings to automatically load a configuration file when the system boots: <ul style="list-style-type: none"> <li>• <b>usb:</b> load the configuration file at boot from an USB mass storage device</li> </ul>

*Table continues...*

Variable	Description
	<ul style="list-style-type: none"> <li>• <b>tftp</b>: load the ASCII configuration file at boot from a TFTP server</li> <li>• <b>sftp</b>: load the ASCII configuration file at boot from a SFTP server</li> <li>• <b>bootp</b>: load the ASCII configuration file at boot and use BootP to obtain values for the TFTP address and file name</li> </ul>
unit <1-8>	The number of the unit in which the USB mass storage device is inserted in.
tftp	Retrieve the configuration from a TFTP server.
sftp	Retrieve the configuration from a SFTP server.
address <A.B.C.D   WORD>	Specifies the address of the SFTP or TFTP server: <ul style="list-style-type: none"> <li>• A.B.C.D—specifies the IPv4 address.</li> <li>• WORD—specifies the IPv6 address.</li> </ul>
filename <WORD>	The name of the configuration file to use in this process.
username <WORD>	Specifies the username.

## View the USB Files

### About this task

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

### Procedure

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

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

3. Press Enter.

### Variable definitions

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

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

## View the USB Host Port Information

### About this task

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

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show usb-host-port [unit <1-8>]`
3. Press Enter.

### Variable definitions

The following table describes the variables for the `show usb-host-port` command.

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

## View the FLASH Files

Use this procedure to view information about the FLASH capacity and current usage. You can display FLASH information on both single and stacked switches. You can also display FLASH information for a specific unit.

### Procedure

1. Enter global configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:  
`show flash [unit <1 - 8>]`
3. Press Enter.

### Example

The following is an example output for a single unit.

```
Switch(config)#show flash
-----
FLASH Memory Usage :
-----
Section                Version                Bytes Used    Bytes Allocated
-----
Total Flash:                ver. 0.0.0.2c                524288        134217728
Boot Image:                 ver. 0.0.0.2c                5802956       524288
Diag Image:                 ver. 7.0.0.090              16286508      8388608
Primary Image:              ver. 7.0.0.076              16256040      33554432
Secondary Image:            ver. 7.0.0.076              16256040      33554432
```

```

Binary Conf:          772096          4194304
Auxiliary Conf:      772096          4194304
Reserved Space:
Available Space:     36962304       36962304
-----

```

## Variable definitions

The following table describes the variables for the `show flash` command.

Variable	Description
unit <1 –8 >	Provides information from the specified unit 1 to 8. DEFAULT: 1

## View FLASH History

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

### Procedure

1. Enter global configuration mode:

```
enable
configure terminal
```
2. At the command prompt, enter the following command:

```
show flash history [unit <1 - 8>]
```
3. Press Enter.

### \* Note:

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

### Example

The following is an example for the `show flash history` command for a single unit.

```

FLASH Write History Unit:
-----
Section                                     Number of writes
-----
Diagnostics Image:                          7
Primary Image:                               44
Secondary Image:                             28
Config Area 1:                              1,345
Config Area 2:                               99
Auxiliary Config Area:                       1,444
MCFG Block :                                4,568
Audit log Area:                              77,123
-----
* Number of minimum guaranteed writes: 100 000
-----

```

## Example

The following is an example for stacked units.

```
FLASH Write History Unit 1:
-----
Section                                     Number of writes
-----
Diagnostics Image:                          17
Primary Image:                               54
Secondary Image:                             10
Config Area 1:                              1,649
Config Area 2:                               199
Auxiliary Config Area:                      1,848
MCFG Block :                                6,569
Audit log Area:                             68,345
-----
* Number of minimum guaranteed writes: 100 000
-----

FLASH Write History Unit 2:
-----
Section                                     Number of writes
-----
Diagnostics Image:                          10
Primary Image:                               24
Secondary Image:                             19
Config Area 1:                              2,567
Config Area 2:                               20
Auxiliary Config Area:                      2,587
MCFG Block :                                5,179
Audit log Area:                             98,978
-----
* Number of minimum guaranteed writes: 100 000
-----
```

## Variable definitions

The following table describes the variables for the `show flash history` command.

Variable	Description
unit <1 –8 >	Provides information from the specified unit 1 to 8. DEFAULT: 1

## Display the Ramdisk Files

Use this procedure to display a list of files in the root directory of the ramdisk or the specified directory.

### Procedure

1. To enter User EXEC mode, log on to the switch.
2. Enter the following command:

```
show ramdisk-files [ascii <filename>] [binary <filename>] [dir
<directoryname>] [tree]
```

## Variable definitions

Use the data in the following table to use the `show ramdisk-files` command.



Variable	Value
ascii	Displays ASCII files.
binary	Displays binary files.
dir	Displays ramdisk directory.
tree	Displays ramdisk tree.
<filename>	Displays the path and name of the file.
<directoryname>	Displays the path and the name of the directory.

## Delete the Ramdisk Files

Use the following procedure to delete all files in the ramdisk.

### Procedure

1. Enter Privileged EXEC mode:  
enable
2. Enter the following command:  
clear ramdisk-files

### Example

```
Switch>enable
Switch#clear ramdisk-files
```

## Download the Ramdisk Files

Use the following procedure to download a specific file type from ramdisk.

### Procedure

1. Enter Privileged EXEC mode:  
enable
2. Enter the following command:  
download ramdisk {diag <filename> | [primary | secondary] image  
<filename> | [primary | secondary] image-if-newer <filename>}

## Variable Definitions

Use the data in the following table to use the **download ramdisk** command.

Variable	Value
diag	Specifies the diagnostics image filename.
image	Specifies the software image filename.
image-if-newer	Specifies the newer software image filename.
poe_module_image	Specifies the POE module image to download.

*Table continues...*

Variable	Value
primary	Specifies the primary agent image to download.
secondary	Specifies the secondary agent image to download.
<filename>	Displays the path and name of the file.

**\* Note:**

For ERS 5928MTS-uPWR hardware, you can use the following command to download the phy firmware: `download ramdisk phy_firmware <filename>`.

## Copy running Configuration on Ramdisk

Use the following procedure to copy running configuration in a specified file on ramdisk.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Enter the following command:

```
copy running-config ramdisk [verbose] [module <module>] filename
<filename>
```

### Variable definitions

Use the data in the following table to use the `copy running-config ramdisk` command.

Variable	Value
verbose	Copies the entire configuration (defaults and non-defaults).
module	Copies the configuration of an application.
filename	Specifies the filename in which to store configuration on ramdisk.
<filename>	Specifies the name of the file.
<module>	Specifies the name of the application module.

## Copy the Files from Ramdisk

Use the following procedure to copy configuration or license files from ramdisk to local configuration.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Enter the following command:

```
copy ramdisk { config <filename> | license <filename>}
```

## Variable definitions

Use the data in the following table to use the `copy ramdisk` command.

Variable	Value
config	Specifies the file to copy to local configuration.
license	Specifies the license to copy from ramdisk
<filename>	Specifies the name of the configuration file or license.

## Load Configuration from Ramdisk

Use the following procedure to load configuration from a file saved on ramdisk.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Enter the following command:

```
configure ramdisk filename <filename>
```

## Variable definitions

Use the data in the following table to use the `configure ramdisk` command.

Variable	Value
filename <filename>	Specifies the filename of the configuration file.

## Copy Configuration in a File on Ramdisk

Use the following procedure to copy configuration in a specified file on ramdisk.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Enter the following command:

```
copy config ramdisk filename <filename>
```

## Variable definitions

Use the data in the following table to use the `copy config ramdisk` command.

Variable	Value
filename <filename>	Specifies the filename on ramdisk from which to copy the configuration.

## Configuring Terminal Settings

You can customize switch terminal settings to suit the preferences of a switch administrator.

### About this task

Use this procedure to configure terminal settings. These settings include terminal length and terminal width.

### Procedure

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

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

3. Press Enter.

#### Important:


Once you modify the terminal configuration, the new settings are applied to the current active session and to all future sessions (serial, telnet or ssh). Concurrent sessions already opened when the terminal configuration was changed, will not be affected.

The terminal setting are saved across login sessions. To change the terminal length and width to the default values, use the `default terminal` command from the Global Configuration command mode. The `default terminal length` command sets the length to 23 lines, and the `default terminal width` command sets the width to 79 characters.

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

## Variable Definitions

The following table describes the variables for the `terminal` command.

Variable	Description
length	Set the length of the terminal display in lines; the default is 23.   <b>Important:</b> If you set the terminal length to 0, the pagination is disabled and the display scrolls continuously.
speed	Set the transmit and receive speeds, the default is 9600.
width	Set the width of the terminal display in characters; the default is 79.

## Set Telnet Access

### About this task

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

### ! Important:

Multiple users can simultaneously access CLI system through the serial port, a telnet session, 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 the switch simultaneously.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command to configure telnet connection:

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

3. **(Optional)** At the command prompt, enter the following command to disable the telnet connection:

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

4. **(Optional)** At the command prompt, enter the following command to set the telnet settings to the default values:

```
default telnet-access
```

## Variable Definitions


The following table describes the variables for the `telnet-access` command.

Variable	Description
enable   disable	Enables or disable telnet connection.
login-timeout <1-10>	Specifies the time in minutes for establishing the telnet connection after the user connects to the switch. Enter an integer from 1–10.
retry <1-100>	Specifies the number of times the user can enter an incorrect password before the connection closes. Enter an integer from 1–100. Default value is 0.

*Table continues...*

Variable	Description
inactive-timeout <0-60>	Specifies the duration in minutes before an inactive session terminates.
logging {none   access   failures   all}	Specifies the events for which you want to store details in the event log: <ul style="list-style-type: none"> <li>• none: Do not save access events in the log.</li> <li>• access: Save only successful access events in the log.</li> <li>• failure: Save failed access events in the log.</li> <li>• all: Save all access events in the log.</li> </ul>
[source-ip <1-50> <XXX.XXX.XXX.XXX> [mask <XXX.XXX.XXX.XXX>]	Specifies the source IP address from which connections can occur. Enter the IP address in dotted-decimal notation. Mask specifies the subnet mask from which connections can occur. Enter the IP mask in dotted-decimal notation.

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

Variable	Description
source-ip [<1-50>]	Disables the Telnet access.  When you do not use the optional parameter, the source-ip list is cleared, which means the first index is 0.0.0.0/0.0.0.0 and the second to fiftieth indexes are 255.255.255.255/255.255.255.255. When you specify a source-ip address, the specified pair is 255.255.255.255/255.255.255.255.   <b>Important:</b>  These same source IP addresses are in the IP Manager list. For more information about the IP Manager list, see Chapter 3.

## Set Boot Parameters

### About this task

Use this procedure to boot the switch or stack and to set boot parameters. This command is used to perform a soft-boot of the switch or stack.

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:

```
boot [primary | secondary ] [default [unit <1-8> ] | nvram block <1-2> | partial-default | script block <1-2> | unit <1-8>]
```

### 3. Press Enter.

#### **!** Important:

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

#### **!** Important:

When you reset the switch or stack to factory partial-default, the switch or stack retains the following settings from the previous configuration:

- IP information
  - IP address
  - subnet mask
  - default gateway
  - bootp mode
  - last bootp IP address
  - last bootp subnet mask
  - last bootp gateway
  - IPV6 management interface address
  - IPV6 default gateway
- software license files
- passwords for console and Telnet/WEB
- SPBM Global Enable state


RADIUS and TACACS authentication settings are not retained. If the console password type is set to local, RADIUS, or TACACS+, after reset, the console password type is set to local.

## Variable Definitions

The following table describes the variables for the `boot` command.

Variables	Description
default	Restores switch or stack to factory-default settings after rebooting.
nvram block <1-2>	Reboots with the binary configuration data in NVRAM using the block specified.
partial-default	Reboots the stack or switch and use factory partial-default configurations.

*Table continues...*

Variables	Description
	<p> <b>Note:</b></p> <p>You can use the boot partial-default command on a standalone switch or on an entire stack. You cannot reset individual units in a stack to partial-default.</p>
primary	Reboots the stack or switch using the primary agent image.
secondary	Reboots the stack or switch using the secondary agent image.
script block <1–2>	Reboots with the ASCII configuration file using the binary configuration block specified.
unit <unit no>	Specifies which unit of the stack is rebooted. This command is available only in stack mode. Enter the unit number of the switch you want to reboot.

## View the Agent and Image Software Load Status

### About this task

Use the following command to display the currently loaded and operational software status for agent and image loads, either individually or combined, for an individual switch or a stack.

### Procedure

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

```
show boot [diag | image [primary | secondary]]
```
3. Press Enter.

### Example

The following is an example of the `show boot` command output.

```
Switch>show boot
Unit  Agent Image Secondary Image Active Image Diag Image Active Diag
-----
1*    7.0.0.042  7.0.0.076      7.0.0.076   0.0.0.2c   0.0.0.2c
* - Unit requires reboot for new Active Image to be made operational.
# - Unit requires reboot for new Diag to be made operational.
```

The following is an example of the `show boot diag` command output.

```
Switch>show boot diag
Unit  Diag Image Active Diag
-----
1     0.0.0.2c  0.0.0.2c
# - Unit requires reboot for new Diag to be made operational.
```

The following is an example of the `show boot image` command output.

```
Switch>show boot image
Unit  Agent Image Secondary Image Active Image
-----
```



```
1*    7.0.0.042    7.0.0.076    7.0.0.076
* - Unit requires reboot for new Active Image to be made operational.
```

The following is an example of the `show boot image primary` command output.

```
Switch>show boot image primary
Unit  Agent Image Active Image
-----
1*    7.0.0.042    7.0.0.076
* - Unit requires reboot for new Active Image to be made operational.
```

The following is an example of the `show boot image secondary` command output.

```
Switch>show boot image secondary
Unit  Secondary Image Active Image
-----
1*    7.0.0.076    7.0.0.076
* - Unit requires reboot for new Active Image to be made operational.
```

The following is an example of the `show boot` command output for a stack.

```
Switch>show boot
Unit  Agent Image Secondary Image Active Image Diag Image Active Diag
-----
1     7.0.0.101    7.0.0.075    7.0.0.101    7.0.0.26    7.0.0.26
2     7.0.0.101    7.0.0.075    7.0.0.101    7.0.0.26    7.0.0.26
3     7.0.0.101    7.0.0.075    7.0.0.101    7.0.0.26    7.0.0.26
4     7.0.0.101    7.0.0.075    7.0.0.101    7.0.0.26    7.0.0.26
* - Stack requires reboot for new Active Image to be made operational.
# - Stack requires reboot for new Diag to be made operational
```

## Variable definitions

Use the data in the following table to use the `show boot` command.

Variable	Definition
diag	Displays information about the diag images.
image	Displays information about images.
primary	Shows primary image software version.
secondary	Shows secondary image software version.

## Configuring BootP

The BootP, DHCP or Default IP mode (the default mode) operates as follows:

- After the switch is reset or power cycled, if the switch is configured with an IP address other than 0.0.0.0 or the default IP address, then the switch uses the configured IP address.
- If the configured IP address is 0.0.0.0 or the default IP address is 192.168.1.1/24, then the switch attempts BootP for 1 minute.
- If BootP succeeds, then the switch uses the IP information provided.
- If BootP fails, the switch attempts to obtain a DHCP IP address.
- If DHCP fails too, and the configured IP address is the default, then the switch uses the default IP address (192.168.1.1/24).

- If BootP fails and the configured IP address is 0.0.0.0, then the switch retains this address.

Use the information in this section to configure BootP parameters.

## Change the BootP Value

### About this task

Use this procedure to change the value of BootP from the default value, which is Default IP. The `ip bootp server` command configures BootP on the current instance of the switch or server.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```


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

```
ip bootp server {always | disable | last | default-ip}
```

3. Press Enter.

### Variable Definitions

Use the data in the following table to use the `ip bootp server` command.

Variable	Definition
always   disable   last   default-ip	<p>Specify 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>• default-ip: Use BootP or the default IP.</li> </ul> <p> <b>Note:</b> The default value is to use default-ip.</p>

## Disable the BootP/DHCP Server

### About this task

Use this procedure to disable the BootP/DHCP server.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
no ip bootp server
```

3. Press Enter.

## Reset the BootP Value

### About this task

Use this procedure to reset the BootP value to Default IP.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
default ip bootp server
```
3. Press Enter.

---

## Customizing the CLI Logon Banner

Use the information in this section to customize the CLI logon banner.

## Display the CLI Banner

### About this task

Use this procedure to display the CLI banner

### Procedure

1. Enter Privileged EXEC mode:
 

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

```
show banner [static | custom]
```
3. Press Enter.

### Variable definitions

Use the data in the following table to use the `show banner` command.

Variable	Definition
static   custom	Specify which banner is currently set to be displayed: <ul style="list-style-type: none"> <li>• static</li> <li>• custom</li> </ul>

## Configure the CLI Logon Banner

### About this task

Use this procedure to configure the CLI logon banner to display a warning message to users before authentication.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `banner` command.

Variable	Definition
static	Activates static banner.
custom	Activates the custom banner.
<line number>	Specifies the banner line number you are setting. The range is 1–19.
<LINE>	Specifies the characters in the line number.
disabled	Skips the banner display.

## Reset the CLI Logon Banner

### About this task

Use this procedure to clear all lines of a previously stored custom banner and to set the banner type to the default setting (static).

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
no banner
```

3. Press Enter.

## Display Help Text on CLI Commands

### About this task

Use this procedure to obtain help on the navigation and use of the Command Line Interface (CLI). You can also request Help at any point by entering a question mark after a command, which shows the available options.

### Procedure

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

```
help [commands mode][application | config | current | dhcp-guard |
exec | ifconfig | interface {Ethernet | loopback | mgmt | vlan} |
privExec |ra-guard | router {isis | ospf | rip | vrrp}] [modes]
```

#### \* Note:

You can use this command in any mode.

3. Press Enter.

## Variable definitions

Use the data in the following table to use the `help` command.

Variable	Definition
commands	Displays commands available by mode. A short explanation of each command is also included.
modes	Displays available modes with information about how to enter each mode.
application	Displays commands available in Application Configuration Mode
config	Displays commands available in Global Configuration Mode
current	Displays commands available in current configuration mode
dhcp-guard	Displays commands available in DHCP-Guard Mode
exec	Displays commands available in executive mode
ifconfig	Displays commands available in Interface Configuration Mode
interface	Displays commands available in Interface Configuration Modes
privExec	Displays commands available in Privileged Executive Mode
ra-guard	Displays commands available in RA-Guard Mode
router	Displays commands available in Router Configuration Modes

## Configuring Auto Unit Replacement

Use the information in this section to configure Auto Unit Replacement (AUR).

## Configure AUR

### About this task

Configure AUR on the switch.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. Enable AUR on the switch.  
`stack auto-unit-replacement enable`
3. Display the AUR settings.  
`show stack auto-unit-replacement`
4. **(Optional)** Restoring default AUR settings.  
`default stack auto-unit-replacement enable`
5. **(Optional)** Disabling the AUR settings.  
`no stack auto-unit-replacement enable`

## Configure AUR Automatic Configuration Save

### About this task

Configure automatic configuration saves for non-base units.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. Enable the automatic configuration saves.  
`stack auto-unit-replacement config save enable`
3. Saving AUR configuration.  
`stack auto-unit-replacement config save unit <1-8>`
4. **(Optional)** Disable AUR automatic configuration saves.  
`stack auto-unit-replacement config save disable`
5. **(Optional)** Restore AUR saved configuration.  
`stack auto-unit-replacement config restore unit <1-8>`

**\* Note:**

Use the base unit console to enter this command.

---

## Managing and Configuring Agent Auto Unit Replacement

Use the information in this section to manage and configure Agent Auto Unit Replacement (AAUR). You can currently manage this functionality only through CLI.

### Enable AAUR

#### About this task

Use this procedure to enable AAUR. Because AAUR is enabled by default, use this command only if this functionality was previously disabled.

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

#### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
stack auto-unit-replacement-image enable
```
3. Press Enter.

### Disable AAUR

#### About this task

Use this procedure to disable AAUR. Because AAUR is enabled by default, you must run this command if you do not want AAUR functionality on a switch.

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

#### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
no stack auto-unit-replacement-image enable
```
3. Press Enter.

## Restore Default AAUR Functionality

### About this task

Use this procedure to set the AAUR functionality to the factory default of enabled.

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

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
default stack auto-unit-replacement-image enable
```
3. Press Enter.

## Display the AAUR Configuration

### About this task

Use this procedure to view the current status of the AAUR functionality.

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

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
show stack auto-unit-replacement-image
```
3. Press Enter.

---

## Configure Stack Forced Mode

### About this task

Use this procedure to configure Stack Forced Mode on a two unit stack.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```



```
configure terminal
```

- At the command prompt, enter the following command:

```
[no | default | show] stack forced-mode
```

- Press Enter.

## Variable definitions

Use the data in the following table to use the `stack forced-mode` command.

Variable	Definition
<code>stack forced-mode</code>	Enables Stack Forced Mode.
<code>no stack forced-mode</code>	Disables Stack Forced Mode.
<code>default stack forced-mode</code>	Restores the default setting for Stack Forced Mode.
<code>show stack forced-mode</code>	Displays 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>

---

## Display Stack Cable Information

### About this task

Use this procedure to obtain the cable information for a stack.

### Procedure

- To enter User EXEC mode, log on to the switch.
- At the command prompt, enter the following command:

```
show stack-cable-info
```

- Press Enter.

---

## Display Complete GBIC Information

### About this task

Use this procedure to obtain complete information for a GBIC port.

**Procedure**

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

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

**\* Note:**

If no GBIC is detected, this command shows no information.

3. Press Enter.

**Variable definitions**

Use the data in the following table to use the `gbic-info` command.

Variable	Definition
<port-list>	Specifies the GBIC port or list of ports for which to display information.

**Display Hardware Information****About this task**

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

**\* Note:**

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

**Procedure**

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show system [verbose]
```

3. Press Enter.

**Variable definitions**

Use the data in the following table to use the `show system` command.

Variable	Definition
[verbose]	Displays additional information about fan status, power status, and switch serial number.

## Shut Down a Switch

### About this task

Use this procedure to safely shut down a switch or stack without interrupting a process or corrupting the software image.

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

While existing CLI sessions do not receive a warning message, all subsequent CLI sessions display the following message: The shutdown process is in progress. It is safe to poweroff the stack. Configuration changes will not be saved. Shutdown has blocked the flash. Autoreset in <xxxx> seconds.

EDM does not receive any shutdown warning messages.

### \* Note:

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

3. Press Enter.

4. The following message appears: Shutdown (y/n) ? Enter yes.

## Variable definitions

Use the data in the following table to use the `shutdown` command.

Variable	Definition
force	Forces the shutdown without confirmation prompt.
minutes-to-wait <1-60>	Specifies the number of minutes that pass before the switch resets itself. The default wait time is 10 minutes.
cancel	Cancels all scheduled switch shutdowns.

---

## Reload Remote Devices

### About this task

Use this procedure to temporarily disable the autosave feature for a specified time period, so you can make configuration changes on remote switches without affecting the currently saved configuration. For example, if you make an error while executing the dynamic switch configuration commands that results in loss of switch connectivity (such as an error in the IP address mask, in the Multi-Link Trunking configuration, or in VLAN trunking), the `reload` command provides you with a safeguard. When the reload timer expires, the switch reboots to the last saved configuration, and connectivity is re-established. Consequently, you need not travel to the remote site to reconfigure the switch.

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

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

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

 **Note:**

Initiate the reload command before you start the switch configuration commands.

3. Press Enter.
4. The following message appears: `Reload (y/n) ?`. Enter `yes`.

### Example

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

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

## Variable definitions

Use the data in the following table to use the `reload` command.

Variable	Definition
force	Forces the reload without confirmation.
minutes-to-wait <1-60>	Specifies the number of minutes that pass before the switch resets itself. The default wait time is 10 minutes.
cancel	Cancels all scheduled switch reloads.

---

## Restore the Factory Default Configuration

### About this task

Use this procedure to reset the switch or stack NVRAM blocks back to the default configuration. The first NVRAM block will be active after the switch and stack resets.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
restore factory-default [-y]
```
3. Press Enter.

## Variable definitions

Use the data in the following table to use the `restore factory-default` command.

Variable	Definition
[-y]	Instructs the switch not to prompt for confirmation.

---

## Viewing IPv4 Socket Information

Use the following procedures to view the IPv4 information.

### Display Information for TCP and UDP Connections

#### About this task

Use the following procedure to display the IPv4 socket information for TCP and UDP connections.

#### Procedure

1. Enter Global Configuration mode:

## System Configuration

```
enable
configure terminal
```

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

```
show ip netstat
```

3. Press Enter.

### Example

The following example shows the results of the `show ip netstat` command

```
Switch(config)#show ip netstat
Proto Recv-Q Send-Q Local Address           Foreign Address         State
-----
TCP      0      0 0.0.0.0.23             0.0.0.0.0              LISTEN
TCP      0      0 0.0.0.0.80             0.0.0.0.0              LISTEN
TCP      0     82 192.0.2.24.23         198.51.100.0.56518    ESTABLISHED
UDP      0      0 0.0.0.0.161           0.0.0.0.0
UDP      0      0 0.0.0.0.0              0.0.0.0.0
UDP      0      0 0.0.0.0.0              0.0.0.0.0
UDP      0      0 192.0.2.24.3491      0.0.0.0.0

Proto Port  Service
-----
TCP    23    TELNET
TCP    80    HTTP
UDP    161   SNMP
UDP    3491  RADIUS
```

## Display Information for TCP Connections

### About this task

Use this procedure to display the IPv4 socket information for TCP connections.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
show ip netstat tcp
```

3. Press Enter.

### Example

The following example shows the results of the `show ip netstat tcp` command.

```
Switch(config)#show ip netstat tcp
Proto Recv-Q Send-Q Local Address           Foreign Address         State
-----
TCP      0      0 0.0.0.0.23             0.0.0.0.0              LISTEN
TCP      0      0 0.0.0.0.80             0.0.0.0.0              LISTEN
TCP      0     82 192.0.2.24.23         198.51.100.0.56518    ESTABLISHED

Proto Port  Service
```

```
-----
TCP    23    TELNET
TCP    80    HTTP
```

## Display Information for UDP Connections

### About this task

Use this procedure to display the IPv4 socket information for UDP connections.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
show ip netstat udp
```
3. Press Enter.

### Example

The following example shows the results of the show ip netstat udp command.

```
Switch(config)#show ip netstat udp
Proto Recv-Q Send-Q Local Address          Foreign Address        State
-----
UDP          0      0 0.0.0.0.161           0.0.0.0.0
UDP          0      0 0.0.0.0.0             0.0.0.0.0
UDP          0      0 0.0.0.0.0             0.0.0.0.0
UDP          0      0 192.0.2.24.3491      0.0.0.0.0
-----
Proto Port  Service
-----
UDP   161   SNMP
UDP   3491  RADIUS
```

## Configuring IPv6

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

Use the following procedures to configure IPv6.

### Enable IPv6 Interface on the Management VLAN

#### About this task

Enable an IPv6 interface on the management VLAN.

#### Procedure

1. Enter VLAN Interface Configuration mode:
 

```
enable
```

- ```
configure terminal
interface vlan <1-4094>
```
2. Enable IPv6 interface.  

```
ipv6 interface enable
```
  3. Enter `exit` to return to the main menu.
  4. Enable IPv6.  

```
ipv6 enable
```

### Variable definitions

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

**Table 15: IPv6 variables and definitions**

| Variable | Definition                    |
|----------|-------------------------------|
| enable   | Default admin status: disable |

## Configure IPv6 Interface on the Management VLAN

### About this task

Assigns an IPv6 address to a VLAN.

### Procedure

1. Enter VLAN Interface Configuration mode:  

```
enable
configure terminal
interface vlan <1-4094>
```
2. Enable IPv6 interface.  

```
ipv6 interface enable
```
3. Return to the main menu.  

```
exit
```

## Display the IPv6 Interface Information

### About this task

Displays the IPv6 interface information.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display IPv6 interface information.



```
show ipv6 interface
```

### Example

```
Switch>enable
Switch#show ipv6 interface
=====
Interface Information
=====
IFINDEX VID/LID  MTU  PHYSICAL          ADMIN  OPER  RCHBLE  RETRAN  TYPE
          ADDRESS          STATE  STATE  TIME    TIME
-----
10001  1      1500 fc:a8:41:fb:40:00 enabled up    30000  1000  ETHER
=====
Address Information
=====
INTF     IPV6          TYPE  ORIGIN  STATUS
INDEX  ADDRESS
-----
10001  2001:DB8:0:0:0:0:ffff/64  UNICAST LINKLAYER PREFERRED
1 out of 1 Total Num of Interface Entries displayed.
1 out of 1 Total Num of Address Entries displayed.
```

## Display IPv6 Interface Addresses

### About this task

View IPv6 interface addresses to learn the addresses.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display IPv6 interface addresses.

```
show ipv6 address interface [loopback <1-16> | mgmt | summary | vlan
<1-4094> | <ipv6_address>]
```

### Example

```
Switch>enable
Switch#
=====
Address Information
=====
IPV6          VID/MID/      TYPE  ORIGIN  STATUS
ADDRESS      TID/LID
-----
2001:DB8:0:0:0:0:ffff/64  V-1  UNICAST LINKLAYER PREF
=====
Address Lifetime Information
=====
IPV6          VID/MID/      VALID  PREF
ADDRESS      TID/LID      LIFETIME LIFETIME
-----
2001:DB8:0:0:0:0:ffff/64  V-1  INF    INF
```

STATUS Legend:  
 PREF=PREFERRED, DEPR=DEPRECATED, INV=INVALID, INAC=INACCESSIBLE, UNK=UNKNOWN  
 TENT=TENTATIVE, DUP=DUPLICATE

## Variable definitions

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

| Variable        | Definition                                                                |
|-----------------|---------------------------------------------------------------------------|
| loopback <1-16> | Specifies the loopback for which IPv6 addresses must be displayed.        |
| mgmt            | Displays IPv6 interfaces for the management port.                         |
| vlan <1-4094>   | Specifies a specific VLAN for which the IPv6 addresses must be displayed. |
| <ipv6_address>  | Specifies the IPv6 address and prefix to be displayed.                    |
| summary         | Displays IPv6 interfaces summary.                                         |

The following table shows the field descriptions for this command.

**Table 16: show ipv6 address interface command field descriptions**

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

## Configure an IPv6 Address for a Switch or Stack

### About this task

Configures an IPv6 address for a switch or stack.

## Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure an IPv6 address.

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

## Variable definitions

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

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

## Display the IPv6 Address for a Switch or Stack

### About this task

Displays the IPv6 address for a switch or stack.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display the IPv6 address.

```
show ipv6 address
```

### Example

```
Switch>enable
Switch#show ipv6 address
Switch Address: ::/0
Stack Address:  ::/0
```

## Configure IPv6 Interface Properties

### About this task

Configures the IPv6 interface, creates the VLAN IPv6 interface, and sets the parameters.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
```

```
interface vlan <1-4094>
```

## 2. Configure the IPv6 interface properties.

```
ipv6 interface [address <WORD>][enable][link-local <WORD>][mtu
<1280-9216>][name <WORD>][reachable-time <1-3600000>][retransmit-
timer <0-3600000>][eui <1-3>]
```

## Variable definitions

Use the data in the following table to use the `ipv6 interface` command.

| Variable                     | Definition                                                                                                                                                                                       |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| address <WORD>               | Specifies the address or prefix length.                                                                                                                                                          |
| enable                       | Enables interface admin status.                                                                                                                                                                  |
| link-local <WORD>            | Specifies the identifier.                                                                                                                                                                        |
| mtu <1280-9216>              | Specifies MTU.                                                                                                                                                                                   |
| name <WORD>                  | Description.                                                                                                                                                                                     |
| reachable-time <1-3600000>   | Specifies the reachable time in milliseconds.                                                                                                                                                    |
| retransmit-timer <0-3600000> | Specifies the retransmit timer in milliseconds.                                                                                                                                                  |
| eui <1-3>                    | Specifies the EUI parameter setting. <ul style="list-style-type: none"> <li>• 1 — Eui-not-used</li> <li>• 2 — eui-used-with-ul-component</li> <li>• 3 — eui-used-without-ul-component</li> </ul> |

## Disable IPv6 Interface

### About this task

Disables the IPv6 interface.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <1-4094>
```

2. Disable IPv6.

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

## Configure Global IPv6 Routing Status

### About this task

Configures global IPv6 routing at the switch level. By default, IPv6 routing is disabled.

## Procedure

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. Enable the global IPv6 administrative status:  

```
ipv6 enable
```
3. Enable the IPv6 forwarding:  

```
ipv6 forwarding
```
4. Configure the IPv6 hop-limit:  

```
ipv6 hop-limit <hop-limit>
```
5. **(Optional)** Disable the global IPv6 administrative status:  

```
no ipv6 enable
```
6. **(Optional)** Disable the IPv6 forwarding:  

```
no ipv6 forwarding
```

## Variable definitions

Use the data in the following table to use the `ipv6 hop-limit` command.

| Variable              | Definitions                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------|
| hop-limit <hop-limit> | Specifies the maximum number of hops before packets drop. The valid range is from 0 to 255. |

## Display the Global IPv6 Configuration

### About this task

Displays the IPv6 global configuration.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. Display the IPv6 global configuration.

```
show ipv6 global
```

### Example

```
Switch>show ipv6 global
forwarding                : disabled
default-hop-cnt           : 30
number-of-interfaces      : 4
number-of-tunnels         : 0
admin-status              : disabled
icmp-error-interval       : 1000
icmp-redirect-msg         : disabled
icmp-unreach-msg          : disabled
```

## System Configuration

```
icmp port-unreach      : enabled
icmp addr-unreach     : enabled
multicast-admin-status : disabled
icmp-error-quota      : 50
block-multicast-replies : disabled
autoconfig            : disabled
slow-path-to-cpu      : disabled
ecmp-max-path         : 1
```

### Job aid

The following table describes the default settings for the fields in the `show ipv6 global`.

| Field                   | Default setting |
|-------------------------|-----------------|
| forwarding              | disabled        |
| default-hop-cnt         | 30              |
| number-of-interfaces    | 4               |
| number-of-tunnels       | 0               |
| admin-status            | disabled        |
| icmp-error-interval     | 1000            |
| icmp-redirect-msg       | disabled        |
| icmp-unreach-msg        | disabled        |
| icmp port-unreach       | enabled         |
| icmp addr-unreach       | enabled         |
| multicast-admin-status  | disabled        |
| icmp-error-quota        | 50              |
| block-multicast-replies | disabled        |
| autoconfig              | disabled        |
| slow-path-to-cpu        | disabled        |
| ecmp-max-path           | enabled         |

## Configure an IPv6 Default Gateway

### About this task

Use this procedure to configure an IPv6 default gateway for the switch or stack.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```
2. At the command prompt, enter the following command:

```
ipv6 default-gateway <ipv6_addr>
```
3. Press Enter.

## Variable definitions

Use the data in the following table to use the `ipv6 default-gateway` command.

| Variable    | Definition                                                |
|-------------|-----------------------------------------------------------|
| <ipv6_addr> | Specifies an IPv6 address as the network default gateway. |

## Delete an IPv6 Default Gateway

### About this task

Use this procedure to delete the IPv6 address that was assigned as the default gateway.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
no ipv6 default-gateway
```
3. Press Enter.

## Display the IPv6 Default Gateway

### About this task

Use this procedure to display the IPv6 address for the default gateway.

### Procedure

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

```
show ipv6 default-gateway
```
3. Press Enter.

## Display the IPv6 Default Routers

### About this task

Display the IPv6 address for the default router.

### Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display the default router IPv6 address.
 

```
show ipv6 default-routers
```

## Display the IPv6 Destination Cache

### About this task

Displays IPv6 destination cache information.

### Procedure

1. To enter User EXEC mode, log on to the switch.
2. Display the destination cache information.

```
show ipv6 destinationcache
```

## Configure the IPv6 Neighbor Cache

### About this task

Use this procedure to add a static neighbor cache entry.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `ipv6 neighbor` command.

| Variable       | Definition                                     |
|----------------|------------------------------------------------|
| <ipv6_address> | Specifies the IPv6 address.                    |
| <unit/port>    | Specifies the port on which to add a neighbor. |
| <H.H.H>        | Specifies the MAC address.                     |

## Delete a Static IPv6 Neighbor

### About this task

Use this procedure to remove a static neighbor cache entry.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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



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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `no ipv6 neighbor` command.

| Variable       | Definition                                                           |
|----------------|----------------------------------------------------------------------|
| <ipv6_address> | Specifies the IPv6 address of the neighbor to delete from the cache. |

## Display the IPv6 Neighbor Information

### About this task

Use this procedure to display IPv6 neighbor information.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show ipv6 neighbor [interface {loopback <1-16> | mgmt | tunnel
<1-2147483647> | vlan <1-4094>} | summary | type {dynamic | local |
other | static} | type {dynamic | local | other | static} |
<ipv6_address>]
```

3. Press Enter.

### Example

The following is an example of the `show ipv6 neighbor` command output.

```
Switch(config)#show ipv6 neighbor
```

```
=====
Neighbor Information
=====
NET ADDRESS/ PHYSICAL ADDRESS          PHYS INTF  TYPE      STATE      LAST UPD
-----
2001:DB8:0:0:0:0:0:ffff/2/ 00:11:F9:34:88:00          V-1 LOCAL   REACHABLE  0
2001:DB8:0:0:0:0:0:ffff/3/ 00:01:02:03:04:05          1/5 STATIC REACHABLE  387452
2001:DB8:0:0:0:0:0:ffff/4/ 00:11:f9:34:88:00          V-1 LOCAL   REACHABLE  385251
2001:DB8:0:0:0:0:0:ffff/32/ 00:11:f9:34:88:00    V-1 LOCAL   REACHABLE  385193
```

### Variable definitions

Use the data in the following table to use the `show ipv6 neighbor` command.

| Variable              | Definition                                     |
|-----------------------|------------------------------------------------|
| interface             | Displays entries by interface.                 |
| loopback <1-16>       | Displays entries per loopback IPv6 interfaces. |
| tunnel <1-2147483647> | Displays entries by tunnel.                    |

*Table continues...*

| Variable                          | Definition                                                                                                                                                                                                                                                                       |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vlan <1-4094>                     | Displays entries by VLAN.                                                                                                                                                                                                                                                        |
| summary                           | Displays summary of IPv6 Neighbor Table.                                                                                                                                                                                                                                         |
| type {other dynamic static local} | Specifies the type of mapping as one of the following: <ul style="list-style-type: none"> <li>• dynamic: dynamically learned neighbor</li> <li>• local: local neighbor address</li> <li>• other: other neighbor entry</li> <li>• static: manually configured neighbor</li> </ul> |
| <ipv6_address>                    | Specifies the neighbor IPv6 address.                                                                                                                                                                                                                                             |

## Display IPv6 Interface ICMP Statistics

### About this task

Use this procedure to display IPv6 interface ICMP statistics.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show ipv6 interface icmpstatistics [loopback] <1-16> | [mgmt] |
[tunnel] <1-2147483647> | [vlan] <1-4094>
```

3. Press Enter.

### Example

The following is an example of the **show ipv6 interface icmpstatistics** command output.

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

## Display IPv6 Interface Process-Redirect

### About this task

Display IPv6 interface processing redirect.

**Procedure**

1. To enter User EXEC mode, log on to the switch.
2. Display IPv6 interface processing redirect.

```
show ipv6 interface process-redirect [mgmt] | [vlan <1-4094>]
```

3. Press Enter.

**Example**

```
Switch>show ipv6 interface process-redirect
=====
Process ICMP redirect status
=====
Process ICMP redirect status for IfIndex = 10001
Disabled
```

**Display IPv6 Interface Statistics****About this task**

Use this procedure to display IPv6 interface statistics.

**Procedure**

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show ipv6 interface statistics [loopback <1-16>] | [mgmt] | [tunnel
<1-2147483647>] | [vlan <1-4094>]
```

3. Press Enter.

**Example**

The following is an example of the **show ipv6 interface statistics** command output.

```
Switch(config)# show ipv6 interface statistics
=====
Icmp Stats
=====
IF stats for IfIndex = 10001
InReceives: 0
InHdrErrors: 0
InTooBigErrors: 0
InNoRoutes: 0
InAddrErrors: 0
InUnknownProtos: 0
InTruncatedPkts: 0
InDiscards: 0
InDelivers: 20
<truncated>
```

## Display IPv6 TCP Statistics

### About this task

Use this procedure to display IPv6 TCP statistics.

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show ipv6 tcp`
3. Press Enter.

### Example

The following is an example of the `show ipv6 tcp` command output.

```
Switch(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
```

## Display IPv6 TCP Connections

### About this task

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show ipv6 tcp connections`
3. Press Enter.

## Display IPv6 TCP Listeners

### About this task

Use this procedure to display IPv6 TCP listeners.

**Procedure**

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show ipv6 tcp listener`
3. Press Enter.

**Display IPv6 UDP Statistics****About this task**

Use this procedure to display IPv6 UDP statistics.

**Procedure**

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show ipv6 udp`
3. Press Enter.

**Display IPv6 UDP Endpoints****About this task**

Use this procedure to display IPv6 UDP endpoints.

**Procedure**

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show ipv6 udp endpoints`
3. Press Enter.

**Clear IPv6 Statistics**

Clear all IPv6 statistics if you do not require previous statistics.

**Procedure**

1. To enter User EXEC mode, log on to the switch.
2. Enter the following command to clear all the IPv6 statistics:  
`clear ipv6 statistics all`
3. Enter the following command to clear interface statistics:

```
clear ipv6 statistics interface [general | icmp] [loopback <1-16> |
mgmt | tunnel <1-2147483647> | vlan <1-4094>]
```

4. Enter the following command to clear RIPng statistics:

```
clear ipv6 statistics ripng
```

5. Enter the following command to clear TCP statistics:

```
clear ipv6 statistics tcp
```

6. Enter the following command to clear UDP statistics:

```
clear ipv6 statistics udp
```

---

## Configuring Link-state

The Link-state (LST) tracking feature identifies the upstream and downstream interfaces. The associations between these two interfaces form link-state tracking group. To enable link-state tracking, create a link-state group, and specify the interfaces that are assigned to the link-state group. An interface can be an aggregation of ports, multi link trunks (MLT) or link aggregation groups (LAG). In a link-state group, these interfaces are bundled together.

### Enable Link-State Tracking

#### About this task

Use this procedure to enable link-state tracking group with upstream or downstream interface.

#### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
link-state group <1-2> {{upstream | downstream}> interface
<interface-type><interface-id> | enable}
```

3. Press Enter.

#### Variable definitions

Use the data in the following table to use the `link-state group` command.

| Variable               | Definition                                                                                 |
|------------------------|--------------------------------------------------------------------------------------------|
| link-state group <1-2> | Specifies the link-state group. Only two link-state tracking groups are supported.         |
| upstream   downstream  | Specifies if the set is upstream or downstream and adds the interface to the specific set. |

*Table continues...*

| Variable         | Definition                                                                                                                 |
|------------------|----------------------------------------------------------------------------------------------------------------------------|
| <interface-type> | Specifies the interface type. It can be an aggregation of ports, multi link trunks (MLT) or link aggregation groups (LAG). |
| <interface-id>   | Specifies the interface ID.                                                                                                |
| enable           | Enables the tracking group.                                                                                                |

## Disable Link-State Tracking

### About this task

Use this procedure to disable link-state tracking group with upstream or downstream interface.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
no link-state group <1-2> {{upstream | downstream}} interface
<interface-type><interface-id> | enable}
```

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `no link-state group` command.

| Variable               | Definition                                                                                                                 |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| link-state group <1-2> | Specifies the link-state group. Only two link-state tracking groups are supported.                                         |
| upstream   downstream  | Specifies if the set is upstream or downstream and adds the interface to the specific set.                                 |
| <interface-type>       | Specifies the interface type. It can be an aggregation of ports, multi link trunks (MLT) or link aggregation groups (LAG). |
| <interface-id>         | Specifies the interface ID.                                                                                                |
| enable                 | Enables the tracking group.                                                                                                |

## Assign Default Values to Link-State Tracking

### About this task

Use this procedure to assign default values to link-state tracking.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

- At the command prompt, enter the following command:

```
default link-state group <1-2> [upstream | downstream]
```

- Press Enter.

### Variable definitions

Use the data in the following table to use the `default link-state group` command.

| Variable               | Definition                                                                                 |
|------------------------|--------------------------------------------------------------------------------------------|
| link-state group <1-2> | Specifies the link-state group. Only two link-state tracking groups are supported.         |
| upstream   downstream  | Specifies if the set is upstream or downstream and adds the interface to the specific set. |

## Display Link-State Tracking

### About this task

Use this procedure to view link-state tracking details.

### Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

```
show link-state [group <1-2>] [detail]
```

- Press Enter.

### Variable definitions

Use the data in the following table to use the `show link-state` command.

| Variable               | Definition                                                                         |
|------------------------|------------------------------------------------------------------------------------|
| link-state group <1-2> | Specifies the link-state group. Only two link-state tracking groups are supported. |
| detail                 | Specifies to display detailed tracking group information.                          |

## Job Aid: Sample Configuration

This section provides sample steps for configuring link-state tracking group 1 with ports 1/1, 2/1 and MLT 1 as upstream members and ports 1/2, 2/2 and MLT 2 as downstream members.

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- Set ports 1/1 and 2/1 as upstream interfaces for LST group 1:



- ```
link-state group 1 upstream interface Ethernet 1/1,2/1
```
3. Add MLT 1 to LST group 1 upstream members:
 

```
link-state group 1 upstream interface mlt 1
```
  4. Define ports 1/2 and 2/2 as downstream members for LST group 1:
 

```
link-state group 1 downstream interface Ethernet 1/2, 2/2
```
  5. Add MLT 2 to LST group 1 downstream members:
 

```
link-state group 1 downstream interface mlt 2
```
  6. Enable LST group 1:
 

```
link-state group 1 enable
```

---

## Administering General Switch using the CLI

This section describes the CLI commands used in general switch administration.

### Configuring Multiple Switches

The switch supports the storage of two switch configurations in flash memory. The switch can use either configuration and must be reset for the configuration change to take effect.

A regular reset of the switch synchronizes configuration changes to the active configuration, whereas a reset to defaults sets configuration to factory defaults. The inactive block is not affected.

In stack configurations, all units in the stack must use the same active configuration. If a unit joins a stack, a check is performed between the unit active configuration and the stack active configuration. If the two differ, the new stack unit resets and loads the stack active configuration.

The following considerations apply to NVRAM commands:

- The Nvram block that is not active is not reset to default after downgrade.
- You can save the switch binary configuration to the non-default NVRAM block.
- When you perform an agent code downgrade on the switch, only the configuration from the default block resets to default.

### Display the Stored Configuration

#### About this task

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

#### Procedure

1. Enter Privileged EXEC mode:
 

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

```
show nvram block
```

3. Press Enter.

## Copy a Configuration to Flash Memory

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the command.

Variable	Definition
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 a Configuration from Flash Memory

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

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

#### **Note:**

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

3. Press Enter.

## Configuring System IP Addresses and Boot Mode Information

Use the information in this section to configure, clear, and view IP addresses, gateway addresses, and boot mode information .

### Configure System IP Addresses and Boot Mode

#### About this task

Use this procedure to set the IP address and subnet mask for a switch or a stack, and to select BootP or DHCP as the boot mode for the next switch reboot.

#### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
ip address <A.B.C.D> [netmask <A.B.C.D>] source {bootp-always|bootp-
last-address|bootp-when-needed|configured-address|dhcp-always|dhcp-
last-address|dhcp-when-needed} [stack|switch|unit]
```

If the stack or switch parameter is not specified, the system automatically modifies the stack IP address when in stack mode and modifies the switch IP address when in standalone mode

#### \* Note:

When you change the IP address or subnet mask, connectivity to Telnet and the Web can be lost.

3. Press Enter.

#### Variable definitions

Use the data in the following table to use the `ip address` command.

Variable	Definition
A.B.C.D	Specifies the IP address in dotted-decimal notation.
netmask	Specifies the IP subnet mask for the stack or switch. The netmask is optional.
source	Specifies whether to use the BootP or DHCP server to assign an IPv4 address for the management VLAN at the next switch reboot. Values include: <ul style="list-style-type: none"> <li>• bootp-always—always use the BootP server</li> <li>• bootp-last-address—use the BootP server last used</li> <li>• bootp-when-needed—use the BootP server when needed</li> <li>• configured-address—use configured server IP address</li> </ul>

*Table continues...*

Variable	Definition
	<ul style="list-style-type: none"> <li>• dhcp-always—always use the DHCP server</li> <li>• dhcp-last-address—use the DHCP server last used</li> <li>• dhcp-when-needed—use the DHCP server when needed</li> </ul>
stack   switch   unit	Specifies the IP address and netmask of the stack or the switch, or another unit in at a stack.

## Reset System IP Addresses, Subnet Mask, and Boot Mode

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
default ip address [source]
```

**\* Note:**

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `default ip address` command.

Variable	Definition
source	Configures the BootP and DHCP boot mode to default for the next system reboot.

## Clear the IP Address and Subnet Mask for a Switch or a Stack

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

**\* Note:**

When you change the IP address or subnet mask, connectivity to Telnet and the Web Interface can be lost. Any new Telnet connection can be disabled and must connect to the serial console port to configure a new IP address.

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `no ip address` command.

Variable	Definition
stack   switch	Zeroes out the stack IP address and subnet mask or the switch IP address and subnet mask.
unit	Zeroes out the IP address for the specified unit.

### Display the Boot Mode

#### About this task

Use this procedure to display the configured boot mode for the next switch reboot.

#### Procedure

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

```
show ip address source
```

3. Press Enter.

### Configure DHCP Client Lease Time

#### About this task

Use this procedure to configure the DHCP client lease time in seconds, minutes, hours, days, and weeks.

#### Procedure

1. Enter Global Configuration mode:
 

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:

```
ip dhcp client lease <time>
```

**\* Note:**

When you change the IP address or subnet mask, connectivity to Telnet and the Web can be lost.

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `ip dhcp client lease` command.

Variable	Definition
<time>	<p>Specifies the DHCP client lease time. Values include:</p> <ul style="list-style-type: none"> <li>• seconds—from 10–4294967295</li> <li>• minutes—from 1–71582788</li> <li>• hours—from 1–1193046</li> <li>• days—from 1–49710</li> <li>• weeks—from 1–7101</li> </ul>

## Reset DHCP Client Lease Time

### About this task

Use this procedure to set the DHCP client lease time (seconds, minutes, hours, days, and weeks) to default values.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
default ip dhcp client lease
```

 **Note:**

When you change the IP address or subnet mask, connectivity to Telnet and the Web can be lost.

3. Press Enter.

## Delete the DHCP Client Lease Time

### About this task

Use this procedure to delete the DHCP client lease time.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
no ip dhcp client lease
```

3. Press Enter.

## Display the DHCP Client Lease Time

### About this task

Use this procedure to display the configured and granted DHCP client lease time.

### Procedure

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

```
show ip dhcp client lease
```

3. Press Enter.

## Renew the DHCP Client Lease

### About this task

Use this procedure to renew the DHCP client lease.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:
 

```
renew dhcp
```
3. Press Enter.

## Configure the Default IP Gateway Address for a Switch or a Stack

### About this task

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

### Procedure

1. Enter Global Configuration mode:
 

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:
 

```
ip default-gateway <XXX.XXX.XXX.XXX>
```

#### **Note:**

When you change the IP gateway, connectivity to Telnet and the Web Interface can be lost.

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `ip default-gateway` command.

Variable	Definition
XXX.XXX.XXX.XXX	Specifies the dotted-decimal IP address of the default IP gateway.

## Clear the IP Default Gateway Address

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
no ip default-gateway
```

#### Note:

When you change the IP gateway, connectivity to Telnet and the Web Interface can be lost.

3. Press Enter.

## Display IP Configurations

### About this task

Use this procedure to display the IP configurations, BootP mode, stack address, switch address, subnet mask, and gateway address. The `show ip` command displays these parameters for what is configured, what is in use, and the last BootP. If you do not enter any parameters, this command displays all IP-related configuration information.

### Procedure

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `show ip` command.



Variable	Definition
bootp	Displays BootP-related IP information.
default-gateway	Displays the IP address of the default gateway.
address	Displays the current IP address.

## Configuring IP Addresses for Specific Units

Use the information in this section to assign and clear IP addresses for a specific unit in a stack.

### Assign IP Addresses for a Specific Unit

#### About this task

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

#### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

#### \* Note:

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

3. Press Enter.

#### Variable definitions

Use the data in the following table to use the `ip address unit` command.

Variable	Definition
unit <1—8>	Sets the unit you are assigning an IP address.
A.B.C.D	Enter IP address in dotted-decimal notation.

### Clear the IP Address for a Specific Unit

#### About this task

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

#### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

**\* Note:**

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `no ip address unit` command.

Variable	Definition
unit <1—8>	Zeroes out the IP address for the specified unit.

## Display Interfaces

### About this task

Use this procedure to view the status of all interfaces on the switch or stack, including MultiLink Trunk membership, link status, autonegotiation, and speed.

### Procedure

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

```
show interfaces [admin-disabled] [admin-enabled] [gbic-info] [LINE]
[link-down] [link-up] [loopback <1-16>] [names <portlist>] [verbose]
```

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `show interfaces` command.

Variable	Definition
admin-disabled	Displays the admin disabled interfaces.
admin-enabled	Displays the admin enabled interfaces.
gbic-info	Displays the GBIC details.
LINE	Display a list of existing ports with names (displays interface names).
link-down	Displays the interfaces with the link down.
link-up	Displays the interfaces with the link up.
loopback <1-16>	Displays Loopback interface information.
names <portlist>	Displays the interface names; enter specific ports to see only those ports.
verbose	Displays the port status information for several applications.

## Display Configuration Information for Ports

### About this task

Displays the configuration information for a specific port. You can view information related to port configuration, VLAN interface, VLAN port member, and Spanning-Tree configuration.

### Procedure

1. Enter Privileged EXEC mode:  
enable
2. At the command prompt, enter the following command:  
show interfaces <portlist> [config] [verbose]
3. Press Enter.

### Example

The following example displays sample output for the **show interfaces <portlist> config** command:

```
Switch#show interfaces 1 config
Port: 1
  Trunk:
  Admin Status:  Enable
  Oper Status:   Down
  EAP Oper Status: Up
  VLACP Oper Status: Down
  STP Oper Status: Forwarding
  Link: Down
  Last Change: 1 day(s), 17h:59m:26s ago
  LinkTrap: Enabled
  Link Autonegotiation: Enabled
  Energy Saver: Disabled
  Energy Saver Oper Status: No Power Saving
  BPDU-guard (BPDU Filtering): Disabled
  BPDU-guard (BPDU Filtering) Oper Status: N/A
  SLPP-guard: Disabled
  SLPP-guard Oper Status: N/A

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

*****VLAN ID port member configuration*****
Port  VLAN  VLAN Name      VLAN  VLAN Name      VLAN  VLAN Name
----  -
1     1     VLAN #1

*****Spanning-tree port configurations*****
Port  Trunk  Participation  Priority  Path Cost      State
----  -
1     Normal Learning  128      1         Forwarding
```

The following example displays sample output for the `show interfaces <portlist> verbose` command:

```
Switch#show interfaces 1 verbose
Port: 1
  Trunk:
    Admin Status: Enable
    Oper Status: Down
    EAP Oper Status: Up
    VLACP Oper Status: Down
    STP Oper Status: Forwarding
    Link: Down
    Last Change: 1 day(s), 17h:58m:11s ago
    LinkTrap: Enabled
    Link Autonegotiation: Enabled
    Energy Saver: Disabled
    Energy Saver Oper Status: No Power Saving
    BPDU-guard (BPDU Filtering): Disabled
    BPDU-guard (BPDU Filtering) Oper Status: N/A
    SLPP-guard: Disabled
    SLPP-guard Oper Status: N/A
```

## Variable definitions

Use the data in the following table to use the `show interfaces` command.

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

## Configuring Port Speed

Use the information in this section to set port speed and duplexing.

### Set the Port Speed

#### About this task

Use this procedure to set the port speed.

#### \* Note:

Enabling or disabling autonegotiation for speed also enables or disables it for duplex operation. When you set the port speed for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

#### \* Note:

If you need to establish a 100 Mbps link on an ERS 5928MTS-uPWR port, note that if autonegotiation is enabled on the port and the peer port speed is forced to 100 Mbps (autonegotiation disabled), the link will not be established. By design, the autonegotiation process does not complete successfully in this scenario because the MTS unit is not able to link at half duplex speeds.

To prevent this situation, perform one of the following actions:

- enable autonegotiation on both peers and configure peers to advertise the *100-full* auto-negotiation-advertisement

OR

- disable autonegotiation by forcing the port speed to 100 Mbps full duplex on both peers

## Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
speed [port <portlist>] {10 | 100 | 1000 | 10000 | 2500 | auto}
```

3. Press Enter.

## Variable Definitions

Use the data in the following table to use the `speed` command.

Variable	Definition
port <portlist>	Specifies the port numbers to configure the speed.  * <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the interface command.
10 100 1000 2500 auto	Sets the 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>• 10000: 10000 Mb/s or 10 GB/s</li> <li>• 2500: 2500 Mb/s or 2.5 GB/s</li> <li>• auto: autonegotiation</li> </ul>

## Reset Port Speed

### About this task

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

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```


- At the command prompt, enter the following command:

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

- Press Enter.

### Variable Definitions

Use the data in the following table to use the `default speed` command.

Variable	Definition
port <portlist>	Specifies the port numbers for which to set the speed to factory default.   <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the interface command.

## Initiating and Displaying Results for a cable Diagnostic Test using the CLI

Use the information in this section to initiate and display results for a cable diagnostic test globally, or for one or more specific switch ports, using the Time Domain Reflectometer (TDR).

### Test Cables with TDR

#### About this task

Use this procedure to run a cable diagnostic test globally, or for one or more specific switch ports.

 **Note:**

Extreme Networks does not include a professional level cable tester.

#### Procedure

- Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command:

```
tdr test <portlist>
```

- Press Enter.

### Variable definitions

Use the data in the following table to use the `tdr test` command.

Variable	Definition
<WORD>	Specifies a port or list of ports.

## Display the TDR Test Results

#### About this task

Use this procedure to display cable diagnostic test results globally, or for one or more specific switch ports.

**Procedure**

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show tdr <portlist>`
3. Press Enter.

**Variable definitions**

Use the data in the following table to use the `show tdr test` command.

Variable	Definition
<portlist>	Specifies a port or list of ports.

**Configuring Enterprise Autotopology Protocol**

Use the information in this section to configure the Enterprise Autotopology protocol.

**Enable the Autotopology Protocol****About this task**

Use this procedure to enable the Autotopology protocol.

**Procedure**

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:  
`autotopology`
3. Press Enter.

**Disable the Autotopology Protocol****About this task**

Use this procedure to disable the Autotopology protocol.

**Procedure**

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:  
`no autotopology`

3. Press Enter.

## Reset the Autotopology Protocol

### About this task

Use this procedure to reset Autotopology to the factory default.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
default autotopology
```
3. Press Enter.

## Display Global Autotopology Settings

### About this task

Use this procedure to display the global autotopology settings.

### Procedure

1. Enter Privileged EXEC mode:  

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

```
show autotopology settings
```
3. Press Enter.

## Display the Autotopology NMM Table

### About this task

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

### Procedure

1. Enter Privileged EXEC mode:  

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

```
show autotopology nmm-table
```
3. Press Enter.

## Configuring Flow Control

Use the information in this section to configure the traffic rates on ports.



**\* Note:**

Due to Quality of Service (QoS) interaction, the switch cannot send pause-frames.

**Configure Flow Control****About this task**

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

**\* Note:**

With auto-negotiation enabled, you must use the "auto-negotiation-advertisements" command to set the mode for flow control.

The default value for flowcontrol is asymmetric (asymm-pause-frame for auto-negotiation enabled). When upgrading from an older software version that has symmetric/pause-frame as default, the symmetric/pause-frame settings are changed to asymmetric/asymm-pause-frame.

If you select the auto mode for flow control on a port, make sure that the desired autonegotiation advertisements are set on the port.

**Procedure**

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

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

3. Press Enter.

**Example**

The following is an example of flow control disabling with autonegotiation enabled:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface ethernet 7-8
Switch(config-if)#auto-negotiation-advertisements port 7 1000-full
Switch(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
-----
7
8 10Full      100Full      1000Full      1000Full      AsymmPause
Switch(config-if)#show interfaces 7-8
      Status      Auto
Port Trunk Admin Oper Link Negotiation Speed Duplex Control
-----
7
8      Enable Up Up Custom 1000Mbps Full Disable
      Enable Up Up Enabled 1000Mbps Full Disable
The following is an example of flow control enabling with autonegotiation enabled:
Switch(config-if)#auto-negotiation-advertisements port 7 1000-full asymm-pause-frame
Switch(config-if)#show auto-negotiation-advertisements port 7-8
```

## System Configuration

```
Port Autonegotiation Advertised Capabilities
-----
7                               1000Full           AsymmPause
8      10Full      100Full      1000Full           AsymmPause
Switch(config-if)#show interfaces 7-8
      Status      Auto      Flow
Port Trunk Admin   Oper   Link Negotiation  Speed  Duplex Control
-----
7                               1000Mbps Full  Asymm
8                               1000Mbps Full  Asymm
```

The following is an example of flow control disabling with autonegotiation disabled:


```
Switch(config-if)#speed port 7-8 1000
Switch(config-if)#duplex port 7-8 full
Switch(config-if)#flowcontrol port 7-8 disable
Switch(config-if)#show interfaces 7-8
      Status      Auto      Flow
Port Trunk Admin   Oper   Link Negotiation  Speed  Duplex Control
-----
7                               Disabled 1000Mbps Full  Disable
8                               Disabled 1000Mbps Full  Disable
```

The following is an example of flow control enabling with autonegotiation disabled:

```
Switch(config-if)#flowcontrol port 7-8 asymmetric
Switch(config-if)#show interfaces 7-8
      Status      Auto      Flow
Port Trunk Admin   Oper   Link Negotiation  Speed  Duplex Control
-----
7                               Disabled 1000Mbps Full  Asymm
8                               Disabled 1000Mbps Full  Asymm
```

### Variable Definitions

Use the data in the following table to use the `flowcontrol` command.

Variable	Definition
port <portlist>	Specifies the port numbers to configure for flow control.   <b>Note:</b> If you omit this parameter, the system uses the ports you specified in the interface command but only those ports that have speed set to 1000/full.
asymmetric   auto   disable	Set the mode for flow control: <ul style="list-style-type: none"><li>• asymmetric: PAUSE frames can flow only in one direction (the switch cannot send pause-frames)</li><li>• auto: Enables autonegotiation on the port</li><li>• disable: Disables flow control on the port</li></ul>

### Disable Flow Control

#### About this task

Use this procedure to disable flow control (only on Gigabit Ethernet ports).

**Procedure**


1. Enter Ethernet Interface Configuration mode:  

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:  

```
no flowcontrol [port <portlist>]
```
3. Press Enter.

**Variable Definitions**

Use the data in the following table to use the `no flowcontrol` command.

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

**Reset Flow Control****About this task**

Use this procedure to set the flow control to the default value of automatic, which automatically detects the flow control.

Use the default flowcontrol command only on Gigabit Ethernet ports.

**Procedure**


1. Enter Ethernet Interface Configuration mode:  

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:  

```
default flowcontrol [port <portlist>]
```
3. Press Enter.

**Variable Definitions**

Use the data in the following table to use the `default flowcontrol` command.

Variable	Definition
port <portlist>	<p>Specifies the port numbers for which to default to automatic flow control.</p> <p> <b>Note:</b></p> <p>If you omit this parameter, the system uses the port number you specified in the interface command.</p>

## Configuring Rate-limit

Use the information in this section to limit the percentage of multicast traffic, broadcast traffic, or both.

### Display Rate-limit Information

#### About this task

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

#### Procedure

1. Enter Privileged EXEC mode:
 

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

```
show rate-limit
```
3. Press Enter.

### Configure Rate-limiting on a Port

#### About this task

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

#### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
rate-limit [port <portlist>] {multicast <pct> | broadcast <pct> |
both <pct>}
```
3. Press Enter.

### Variable Definitions

Use the data in the following table to use the `rate-limit` command.

Variable	Definition
port <portlist>	Specifies the port numbers to configure for rate-limiting.  * <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the interface command.
multicast <pct>   broadcast <pct>   both <pct>	Apply rate-limiting to the type of traffic. Enter an integer from 1–10 to set the rate-limiting percentage:  <ul style="list-style-type: none"> <li>• multicast: Apply rate-limiting to multicast packets</li> <li>• broadcast: Apply rate-limiting to broadcast packets</li> <li>• both: Apply rate-limiting to both multicast and broadcast packets</li> </ul>

## Disable Rate-limiting on a Port

### About this task

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

### Procedure

1. Enter Ethernet Interface Configuration mode:  

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:  

```
no rate-limit [port <portlist>]
```
3. Press Enter.

### Variable Definitions

Use the data in the following table to use the `no rate-limit` command.

Variable	Definition
port <portlist>	Specifies the port numbers for which to disable for rate-limiting.  * <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the interface command.

## Reset Rate-limiting

### About this task

Use this procedure to restore the rate-limiting value for specified ports to the default settings.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```


- At the command prompt, enter the following command:

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

- Press Enter.

### Variable Definitions

Use the data in the following table to use the `default rate-limit` command.

Variable	Definition
port <portlist>	Specifies the port numbers for which to reset rate-limiting to factory default.   <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the interface command.

## Configuring Simple Network Time Protocol

Use the information in this section to configure Simple Network Time Protocol (SNTP).

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

### Note:

If problems occur when you use this feature, try various NTP servers. Some NTP servers can be overloaded or currently inoperable.

The system retries connecting with the NTP server a maximum of three times, with 5 minutes between each retry.

## Display SNTP Information

### About this task

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

### Procedure

- Enter Privileged EXEC mode:
 

```
enable
```
- At the command prompt, enter the following command:
 

```
show sntp
```
- Press Enter.

## Display the Current System Characteristics

### About this task

Use this procedure to display the current system characteristics.

**\* Note:**

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

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show sys-info`
3. Press Enter.

## Enable the SNTP

### About this task

Use this procedure to enable SNTP.

**\* Note:**

The default setting for SNTP is Disabled

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:  
`sntp enable`
3. Press Enter.

## Disable the SNTP

### About this task

Use this procedure to disable SNTP.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:

```
no sntp enable
```

3. Press Enter.

## Configure the SNTP Server Primary Address

### About this task

Use this procedure to configure the SNTP server primary address.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `sntp server primary address` command.

Variable	Definition
ipv6_address	Specifies the IPv6 address of the primary NTP server.
<A.B.C.D>	Specifies the IP address of the primary NTP server in dotted-decimal notation.

## Configure the SNTP Server Secondary Address

### About this task

Use this procedure to configure the SNTP server secondary address.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `sntp server secondary address` command.



Variable	Definition
ipv6_address	Specifies the IPv6 address of the secondary NTP server.
<A.B.C.D>	Specifies the IP address of the secondary NTP server in dotted-decimal notation.

## Clear SNTP Addresses

### About this task

Use this procedure to clear the NTP server IP addresses. The `no sntp server` command clears the primary and secondary server addresses.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
no sntp server {primary | secondary}
```
3. Press Enter.

### Variable definitions

Use the data in the following table to use the `no sntp server` command.

Variable	Definition
primary	Clears the primary SNTP server address.
secondary	Clears the secondary SNTP server address.

## Perform a Manual SNTP Synchronization

### About this task

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

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
sntp sync-now
```
3. Press Enter.

## Configure a Recurring Synchronization

### About this task

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

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
sntp sync-interval <0-168>
```
3. Press Enter.

### Variable definitions

Use the data in the following table to use the `sntp sync-interval` command.

Variable	Definition
<0-168>	Specifies the number of hours for periodic synchronization with the NTP server. 0 is boot-time only, and 168 is once a week.

## Configure Local Time Zone

### Before you begin

SNTP server must be enabled.

### About this task

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

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
clock time-zone zone hours [minutes]
```
3. Press Enter.

### Example

The following is an example of setting the time zone to UTP minus 8 hours and displaying the time zone as "PST".

```
Switch(config)#clock time-zone PST -8
```

## Variable definitions

Use the data in the following table to use the `clock time-zone zone hours` command.

Variable	Definition
zone	Specifies the time zone acronym to be displayed when showing system time (up to 4 characters).
hours	Specifies the difference from UTC in hours. This can be any value between -12 and +12.
[minutes]	Specifies the number of minutes difference from UTC. Minutes can be any value between 0 and 59.

## Configure Daylight Savings Time

### Before you begin

SNTP server must be enabled.

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Press Enter.

### Example

The following 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.

```
Switch(config)#clock summer-time BST date 28 Mar 2007 2:00 30 Aug 2007 15:00 +60
```

## Variable definitions

Use the data in the following table to use the `clock summer-time` command.

Variable	Definition
<zone>	Specifies the time zone acronym to display when daylight savings time is in effect. If unspecified, the default is the current time zone acronym.
date	Specifies daylight savings time to start and end on the following dates.

*Table continues...*

Variable	Definition
<day>	Specifies the start day.
<month>	Specifies the start month.
<year>	Specifies the start year.
<hh:mm>	Specifies the hour and minute to start daylight savings time.
<end-day>	Specifies the end day.

## Configure Recurring Daylight Savings Time

### Before you begin

SNTP server must be enabled.

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Press Enter.

### Example

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



```
Switch(config)# clock summer-time recurring 3 13 March 02:00 2 6 November 02:00 offset 60
```

## Variable Definitions

Use the data in the following table to use the `clock summer-time recurring` command.

Variable	Definition
<startWeek:1-5>   last>	<p>Specifies the week of the month (starting on Sunday) you want recurring daylight savings time to start. Values include:</p> <ul style="list-style-type: none"> <li>• &lt;1-5&gt; — the first to the fifth week for months of the year that include five Sundays.</li> <li>• last — the last week of months of the year that do not include five Sundays.</li> </ul>

*Table continues...*

Variable	Definition
	<p> <b>Note:</b></p> <p>For the &lt;1–5&gt; parameter, weeks count from the first day of the month, not calendar weeks. Therefore, weeks 1–4 may not always apply. Week 5 may not apply in certain years. In that case, summer time start/end uses the last parameter.</p> <p>For years without a Sunday in the fifth week of March, summer time starts on the last Sunday of March.</p>
<start:DAY>	Specifies the day recurring daylight savings time starts.
<start:MONTH>	Specifies the month recurring daylight savings time starts.
<start:hh:mm>	Specifies the hour and minutes of the day recurring daylight savings time starts.
<endWeek:1–5>   last>	<p>Specifies the week of the month (starting on Sunday) you want recurring daylight savings time to end. Values include:</p> <ul style="list-style-type: none"> <li>• &lt;1–5&gt; — the first to the fifth week for months of the year that include five Sundays.</li> <li>• last — the last week of months of the year that do not include five Sundays.</li> </ul> <p> <b>Note:</b></p> <p>For the &lt;1–5&gt; parameter, weeks count from the first day of the month, not calendar weeks. Therefore, weeks 1–4 may not always apply. Week 5 may not apply in certain years. In that case, summer time start/end uses the last parameter.</p>
<end:DAY>	Specifies the day recurring daylight savings time ends.
<end:MONTH>	Specifies the month recurring daylight savings time ends.
<end:hh:mm>	Specifies the hour and minutes of the day recurring daylight savings time ends.
offset<1–1440>	Specifies the time change in minutes when daylight savings time starts and ends. The offset is added when daylight savings time begins, and subtracted when daylight savings time ends. Value range is 1 to 1440 minutes.

## Advertising Custom Autonegotiation

Custom Autonegotiation Advertisement (CANA) customizes the capabilities that are advertised. It also controls the capabilities that the switch advertises as part of the auto negotiation process.

Use the information in this section to configure CANA.

### Configure CANA

#### About this task

Use this procedure to configure Custom Autonegotiation Advertisements (CANA) for one or more switch ports.

**\* Note:**

If you need to establish a 100 Mbps link on an ERS 5928MTS-uPWR port, note that if autonegotiation is enabled on the port and the peer port speed is forced to 100 Mbps (autonegotiation disabled), the link will not be established. By design, the autonegotiation process does not complete successfully in this scenario because the MTS unit is not able to link at half duplex speeds.

To prevent this situation, perform one of the following actions:

- enable autonegotiation on both peers and configure peers to advertise the *100-full* auto-negotiation-advertisement

OR

- disable autonegotiation by forcing the port speed to 100 Mbps full duplex on both peers

## Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
auto-negotiation-advertisements [port <portlist>] {10-full | 10-half
| 100-full | 100-half | 1000-full | 10000-full | 2500-full | add|
asymm-pause-frame | none | remove}
```

3. Press Enter.

## Example

The following is an example of setting port 5 to 10 Mb/s and full duplex.

```
Switch(config)#interface ethernet 5
Switch(config-if)#auto-negotiation-advertisements port 5 10-full
```

## Variable definitions

Use the data in the following table to use the `auto-negotiation-advertisements` command.

Variable	Definition
<portlist>	Specifies a port or list of ports for which to configure CANA.
10-full	Advertises 10Mbps full-duplex
10-half	Advertises 10Mbps half-duplex
100-full	Advertise 100Mbps full-duplex
100-half	Advertises 100Mbps half-duplex
1000-full	Advertises 1000Mbps full-duplex
10000-full	Advertises 10000Mbps full-duplex

*Table continues...*

Variable	Definition
2500-full	Advertise 2500Mbps full-duplex
asymm-pause-frame	Advertise the use of asymmetric pause frames
none	Do not advertise during autonegotiation

## Display CANA Information

### About this task

Use this procedure to view the autonegotiation advertisements for a switch.

### Procedure

1. Enter Privileged EXEC mode:  

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

```
show auto-negotiation-advertisements [port <portlist>]
```
3. Press Enter.

### Example

The following is an example of the `show auto-negotiation-advertisements` command output.

```
Switch(config)#show auto-negotiation-advertisements port 9
Port Autonegotiation Advertised Capabilities
-----
9                100Full      1000Full      2500Full AsymmPause
Switch(config)#
```

### Variable definitions

Use the data in the following table to use the `show auto-negotiation-advertisements` command.

Variable	Definition
<portlist>	Specifies a port or list of ports for which to display autonegotiation advertisement configuration information.

## Display Hardware Capabilities

### About this task

Use this procedure to display operational modes for the device.

### Procedure

1. Enter Privileged EXEC mode:  

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `show auto-negotiation-capabilities` command.

Variable	Definition
port <portlist>	Specifies a port or list of ports for which to display autonegotiation advertisement capabilities information.

## Restore CANA to Default

### About this task

Use this procedure to restore CANA to default.

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
default auto-negotiation-advertisements [port <portlist>]
```
3. Press Enter.

### Variable definitions

Use the data in the following table to use the `default auto-negotiation-advertisements` command.

Variable	Definition
port <portlist>	Specifies a port or list of ports for which to restore CANA to default settings. The default setting makes a port advertise all auto negotiation capabilities.

## Disable CANA

### About this task

Use this procedure to disable CANA on one or more ports.

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```



- At the command prompt, enter the following command:

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

- Press Enter.

### Variable definitions

Use the data in the following table to use the `no auto-negotiation-advertisements` command.

Variable	Definition
port <portlist>	Specifies a port or list of ports for which to disable CANA.

## Configure Duplex Operation

### About this task

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

#### \* Note:

Enabling or disabling autonegotiation for speed also enables or disables it for duplex operation. When you set the duplex mode for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

### Procedure

- Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

- At the command prompt, enter the following command:

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

- Press Enter.

### Variable Definitions

Use the data in the following table to use the `duplex` command.

Variable	Definition
port <portlist>	Specifies the port numbers to reset the duplex mode to factory default values. The default value is autonegotiation.  * <b>Note:</b> If you omit this parameter, the system uses the ports you specified in the interface command.
full   half   auto	Sets duplex to • full: full-duplex mode

*Table continues...*

Variable	Definition
	<ul style="list-style-type: none"> <li>• half: half-duplex mode</li> <li>• auto: autonegotiation</li> </ul>

## Reset the Duplex Operation

### About this task

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

### Procedure


1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
default duplex [port <portlist>]
```
3. Press Enter.

### Variable Definitions

Use the data in the following table to use the `default duplex` command.

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

## Connecting to another Switch

Use the information in this section to communicate with another switch while maintaining the current switch connection, by running the `ping` and `telnet` commands.

### Use the Ping Command to Test Communication with another Switch

#### Before you begin

To ping from the local IP address, set the local IP address before you issue the ping command.

#### About this task

Use this procedure to determine whether or not you can establish communication between two switches. The ping command tests the network connection to another network device by sending an Internet Command Message Protocol (ICMP) packet from the local IP address (IPv4 address or, DNS host name) or a specified source IPv4 address. The `ping` command waits for a reply within a

predetermined time period. If the reply arrives within the established timeout interval, the host is considered to be reachable.

## Procedure

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

```
ping {<hostname> | A.B.C.D | <WORD>} [continuous] [count <1-9999>]
[datasize <64-4096>] [debug source {<A.B.C.D> | <WORD>}] [interval
<1-60>] [scopeid {<1-4094> | loopback <1-16> | mgmt}] [source
{<A.B.C.D> | <WORD>}] [timeout <1-120>] [ttl <0-255>] [-t <1-120>]
```

3. Press Enter.

## Variable definitions

Use the data in the following table to use the `ping` command.

### Variable definition

Parameter	Description
<Hostname> or {A.B.C.D}	Specifies the hostname or IP address to ping.
<WORD>	Specifies the IPv6 address to ping.
datasize <64-4096>	Specifies the size of the ICMP packet to be sent within a range of 64 to 4096 bytes.  The range is from 64 to 4096 bytes. By default, the data size is 64 bytes.
count <1-9999>   continuous	Sets the number of ICMP packets to be sent within a range of 1 to 9999 packets. The continuous mode sets the ping running until the user interrupts it by entering Ctrl+C.  By default, the packet count is 5.
timeout   -t <1-120>	Sets the timeout using either the timeout with the <code>-t</code> parameter followed by the number of seconds the switch must wait before timing out. Range is within 1 to 120 seconds.  By default, timeout is 5 seconds.
interval <1-60>	Specifies the number of seconds between transmitted packets within a range of 1 to 60 seconds.  By default, the interval is 1 second.
debug	Provides additional output information such as the ICMP sequence number and the trip time.
source <WORD>	Specifies the source IPv4 address of the outgoing ICMP request message. Must be one of the device's layer 3 active interfaces. If no source address is

*Table continues...*

Parameter	Description
	specified, the address of the interface used to send out the packets is used as the source address.
ttl <0–255>	Specifies the maximum hop limit for the packet. The range is from 0 to 255.
scopeid <1–4094>	Specifies the interface VLAN ID for link-local or multicast addresses. The range is from 1 to 4094. By default, the VLAN ID is 1.
loopback <1–16>	Specifies the Loopback interface. The range is from 1 to 16.
mgmt	Specifies the management port.

## Use Telnet to Communicate with another Switch

### About this task

Use the telnet command to establish communications with another switch during the current CLI session. Communication can be established to only one external switch at a time using the `telnet` command.

### Procedure

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

```
telnet <ipv6_address | dns_host_name | ipv4_address>
```
3. Press Enter.

### Variable definitions

Use the data in the following table to use the `telnet` command.

Variable	Definition
ipv6_address	Specifies the IPv6 address of the unit with which to communicate.
dns_host_name	Specifies the DNS host name of the unit with which to communicate.
ipv4_address	Specifies the IPv4 address of the unit with which to communicate.

## Configuring Domain Name Server (DNS)

Use domain name servers when the switch needs to resolve a domain name (such as `extremenetworks.com`) to an IP address.

Use the information in this section to configure DNS.

### Display DNS-related Information

#### About this task

Use this procedure to display DNS-related information. This information includes the default switch domain name and any configured DNS servers.

**Procedure**

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:  
`show ip dns`
3. Press Enter.

**Configure a Domain Name Server****About this task**

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

**\* Note:**

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

**Procedure**

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:  
`ip domain-name <domain_name>`
3. Press Enter.

**Variable definitions**

Use the data in the following table to use the `ip domain-name` command.

Variable	Definition
<domain_name>	Specifies 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 (.).

**Clear the DNS Domain Name****About this task**

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

**Procedure**

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the command prompt, enter the following command:

```
no ip domain-name
```

3. Press Enter.

## Restore DNS Domain Name to Default

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

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

```
default ip domain-name
```

3. Press Enter.

## Resolve Domain Names to IP Addresses

### About this task

Use this procedure to set the domain name servers the switch uses to resolve a domain name to an IP address. A switch can have up to three domain name servers specified for this purpose.

#### Note:

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

### Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `ip name-server` command.

Variable	Definition
ipv6_address	Specifies the IPv6 address of the domain name server used by the switch.
<ip_address_1>	Specifies the IP address of the domain name server used by the switch.
<ip_address_2>	Optional. Specifies the IP address of a domain name server to add to the list of servers used by the switch.
<ip_address_3>	Optional. Specifies the IP address of a domain name server to add to the list of servers used by the switch.

## Remove Domain Name Servers

### About this task

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.

#### \* Note:

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `no ip name-server` command.

Variable	Definition
<ip_address_1>	Specifies the IP address of the domain name server to remove.
<ip_address_2>	Optional. Specifies the IP address of a domain name server to remove from the list of servers used by the switch.
<ip_address_3>	Optional. Specifies the IP address of a domain name server to remove from the list of servers used by the switch.

## Configuring Serial Security

When enabled, the serial-security feature secures the console interface by logging you out if the serial console is removed from the port.

**\* Note:**

When loading an ASCII configuration file on switch, removing the console cable does not involve a logout event.

Use the information in this section to configure serial security.

## Enable the Serial Security

### About this task

Use this procedure to enable serial security on a switch.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
serial-security enable
```
3. Press Enter.

## Disable the Serial Security

### About this task

Use this procedure to disable serial security on a switch.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
no serial-security enable
```
3. Press Enter.

## Restore Serial Security to Default

### About this task

Use this procedure to restore serial security to default (disabled).

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:



```
default serial-security enable
```

3. Press Enter.

## Display Serial Security Status

### About this task

Use this procedure to display the serial security on the switch.

### Procedure

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

```
show serial-security
```

3. Press Enter.

---

## Configuring LLDP using CLI

The following sections provide procedures to enable and configure Link Layer Discovery Protocol (LLDP) using the CLI.

### Set LLDP Transmission Parameters

#### About this task

Use this procedure to set the LLDP transmission parameters.

#### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
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>] [vendor-specific {call-server | file-  
server}]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `lldp` command.

Variables	Description
tx-interval <5-32768>	Sets the interval between successive transmission cycles.

*Table continues...*

Variables	Description
tx-hold-multiplier <2-10>	Sets the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV.
reinit-delay <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.
med-fast-start <1-10>	Sets value for med-fast-start.
notification-interval <5-3600>	Sets the interval between successive transmissions of LLDP notifications.
vendor-specific {call-server   file-server}	Sets the vendor specific details for advertising the call server or file server details to the IP phones.

## Set LLDP Port Parameters

### About this task

Use this procedure to set the LLDP port parameters.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp port <portlist> [status {rxOnly | txAndRx | txOnly}] [config
notification]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `lldp port` command.

Variables	Description
port <portlist>	Specifies the ports affected by the command.
status {rxOnly   txAndRx   txOnly}	<p>Sets the LLDP transmit and receive status on the ports.</p> <ul style="list-style-type: none"> <li>• rxonly: enables LLDP receive only</li> <li>• txAndRx: enables LLDP transmit and receive</li> </ul> <p>For LLDP support for PoE+, transmission and reception must be enabled.</p> <ul style="list-style-type: none"> <li>• txOnly: enables LLDP transmit only</li> </ul>

*Table continues...*

Variables	Description
config notification	Enables notification when new neighbor information is stored or when existing information is removed. The default value is <i>enabled</i> .

## Set LLDP Media Endpoint Devices (MED)

### About this task

Use this procedure to configure LLDP Media Endpoint Devices (MED) policies for switch ports.

#### \* Note:

As a safeguard, a LLDP-MED Network Policy TLV is not sent in the LLDPDUs if the policy has the vlan-id set to value 0 (priority tagged frames).

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp med-network-policies [port <portList>] {voice|voice-signaling}
[dscp <0-63>] [priority <0-7>] [tagging {tagged|untagged}] [vlan-id
<0-4094>]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `lldp med-network-policies` command.

Variable	Description
port <portlist>	Specifies the port or ports on which to configure LLDP MED policies.
voice	Specifies voice network policy. The default value is 46.
voice-signaling	Specifies voice signalling network policy.
dscp <0-63>	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63. The default value is 46.
priority <0-7>	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. Values range from 0–7. The default value is 6.

*Table continues...*

Variable	Description
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 <0-4094>	<p>Specifies the VLAN identifier for the selected port or ports. Values range from 0–4094 (0 is for priority tagged frames). If you select priority tagged frames, the system recognizes only the 802.1p priority level and uses a value of 0 for the VLAN ID of the ingress port.</p>

## Set the Optional Management TLVs

### About this task

Use this procedure to set the optional Management TLVs to be included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp tx-tlv [port <portlist>] [local-mgmt-addr] [port-desc] [sys-
cap] [sys-desc] [sys-name]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `lldp tx-tlv` command.

Variables	Description
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.
port-desc	The port description TLV. This TLV is enabled by default. This TLV is enabled by default.
port <portlist>	Specifies a port or list of ports.
sys-cap	The system capabilities TLV.
sys-desc	The system description TLV. This TLV is enabled by default.

*Table continues...*

Variables	Description
sys-name	The system name TLV. This TLV is enabled by default.
med	The Media Endpoint Device (MED) for a specific TLV.

## Set the Optional IEEE 802.1 Organizationally-Specific TLVs

### About this task

Use this procedure to set the optional IEEE 802.1 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp tx-tlv [port <portlist>] dot1 [port-protocol-vlan-id
<vlanlist>] [port-vlan-id ] [protocol-identity < [EAP] [LLDP]
[STP]>] [vlan-name <vlanlist>]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `lldp tx-tlv dot1` command.

Variables	Description
port <portlist>	The ports affected by the command.
port-protocol-vlan-id <vlanlist>	The port and protocol VLAN ID TLV.
port-vlan-id	The port VLAN ID TLV.
protocol-identity <[EAP] [LLDP] [STP]>	Protocol Identity TLV
vlan-name <vlanlist>	The VLAN name TLV.

## Set the Optional IEEE 802.3 Organizationally-Specific TLVs

### About this task

Use this procedure to set the optional IEEE 802.3 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
```

```
interface Ethernet <port>
```

- At the command prompt, enter the following command:

```
lldp tx-tlv [port <portlist>] dot3 [link-aggregation] [mac-phy-
config-status] [maximum-frame-size] [mdi-power-support]
```

- Press Enter.

## Variable definitions

The following table describes the variables for the `lldp tx-tlv dot3` command.

Variables	Description
port <portlist>	The ports affected by the command.
link-aggregation	The link aggregation TLV.
mac-phy-config-status	The MAC/Phy configuration or status TLV.
maximum-frame-size	Maximum Frame Size TLV.
mdi-power-support	Power via MDI TLV is sent only on ports where transmission is enabled. The power via MDI TLV, transmission of this TLV is enabled by default on all POE ports. The transmission can be enabled only on PoE ports.

## Set the Optional Organizationally Specific TLVs

### About this task

Use this procedure to set the optional organizationally specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

### Procedure

- Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

- At the command prompt, enter the following command:

```
lldp tx-tlv [port <portlist>] med [extendedPSE] [inventory]
[location] [med-capabilities] [network-policy]
```

- Press Enter.

## Variable definitions

The following table describes the variables for the `lldp tx-tlv med` command.

Variables	Description
port <portlist>	specifies the ports affected by the command

*Table continues...*

Variables	Description
med-capabilities	MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted). This TLV is enabled by default.
extendedPSE	Extended PSE TLV, the transmission of this TLV is enabled by default only on POE port switches.
inventory	Inventory TLVs This TLV is enabled by default.
location	Location Identification TLV This TLV is enabled by default.
network-policy	Network Policy TLV This TLV is enabled by default.

## Set the LLDP Transmission Parameters to Default Values

### About this task

Use this procedure to set the LLDP transmission parameters to their default values.

#### \* Note:

If no parameters are specified, the default lldp sets all parameters to their default parameters.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
default lldp [tx-interval ] [tx-hold-multiplier ] [reinit-delay]
[tx-delay] [notification-interval] [med-fast-start]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `default lldp` command.

Variables	Description
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 re-initialize 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 to the default value.

## Set the Port Parameters to Default Values

### About this task

Use this procedure to set the port parameters to their default values.

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
default lldp port <portlist> [status] [config notification]
```
3. Press Enter.

### Variable definitions

The following table describes the variables for the `default lldp port` command.

Variables	Description
port <portlist>	The ports affected by the command.
status	Sets the LLDP transmit and receive status to the default value (txAndRx).
config notification	Sets the config notification to its default value (disabled).

## Set the LLDP MED Policies to Default Values

### About this task

Use this procedure to set LLDP MED policies for switch ports to default values.

#### \* Note:

If no parameter is used, both voice and voice-signaling lldp network policies are restored to default. Starting with release 5.5, a default network policy for voice id is defined on all switch ports. This have Layer 2 priority 6, DSCP 46, tagging parameter set to untagged and vlan ID 0.

#### \* Note:

As a safeguard, a LLDP-MED Network Policy TLV is not sent in the LLDPDUs, if the policy has the vlan-id set to value 0 (priority tagged frames).

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```



- At the command prompt, enter the following command:

```
default lldp med-network-policies {voice|voice-signaling} [port
<portList>]
```

- Press Enter.

### Variable definitions

The following table describes the variables for the `default lldp med-network-policies` command.

Variable	Description
port <portlist>	Specifies the port or ports on which to configure default LLDP MED policies.
voice	Specifies the default voice network policy. The default value is 46.
voice-signaling	Specifies the default voice signalling network policy.

## Set the LLDP Management TLVs to default values

### About this task

Use this procedure to set the LLDP Management TLVs to their default values.

### Procedure

- Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

- At the command prompt, enter the following command:

```
default lldp tx-tlv port <portlist> local-mgmt-addr port-desc sys-
cap sys-desc sys-name
```

- Press Enter.

### Variable definitions

The following table describes the variables for the `default lldp tx-tlv` command.

Variables	Description
port <portlist>	The ports affected by the command.
port-desc	The port description TLV. This TLV is enabled by default.
sys-name	The system name TLV. This TLV is enabled by default.
sys-desc	The system description TLV. This TLV is enabled by default.
sys-cap	The system capabilities TLV. This TLV is enabled by default.

*Table continues...*

Variables	Description
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.

## Set the Optional IEEE 802.1 and Organize Specific TLVs to Default Values

### About this task

Use this procedure to set the optional IEEE 802.1 organizationally specific TLVs to their default values.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
default lldp tx-tlv port <portlist> dot1 [port-protocol-vlan-id]
[port-vlan-id] [protocol-identity [EAP] [LLDP] [STP]] [vlan-name]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `default lldp tx-tlv dot1` command.

Variables	Description
port <portlist>	The ports affected by the command.
port-vlan-id	The port VLAN ID TLV (default value is false: not included).
vlan-name	The VLAN Name TLV (default value is none).
port-protocol-vlan-id	The port and protocol VLAN ID TLV (default value is none).
protocol-identity [EAP] [LLDP] [STP]	The protocol identity TLV (default value is none).

## Set the Optional IEEE 802.3 and Organize Specific TLVs to Default Values

### About this task

Use this procedure to set the optional IEEE 802.3 organizationally specific TLVs to their default values.

#### Note:

Transmission of MDI TLVs can be enabled only on POE switch ports.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
```

```
configure terminal
interface Ethernet <port>
```

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

```
default lldp tx-tlv port <portlist> dot3 link-aggregation mac-phy-
config-status maximum-frame-size mdi-power-support
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `default lldp tx-tlv dot3` command.

Variables	Description
port <portlist>	The ports affected by the command.
mac-phy-config-status	The MAC/Phy Configuration/Status TLV (default value is false: not included).
mdi-power-support	The power via MDI TLV. This TLV is enabled by default.
link-aggregation	The link aggregation TLV (default value is false: not included).
maximum-frame-size	The maximum frame size TLV (default value is false: not included).

## Set the Default Values for the Optional TLVs for MED Devices

### About this task

Use this procedure to set default values for the optional organizationally specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

#### Note:

Transmission of ExtendedPSE TLVs can be enabled only on POE switch ports.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
default lldp tx-tlv port <portlist> med extendedPSE inventory
inventory location med-capabilities network-policy
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `default lldp tx-tlv med` command.

Variables	Description
port <portlist>	specifies the ports affected by the command
med-capabilities	MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted). This TLV is enabled by default.
extendedPSE	Extended PSE TLV This TLV is enabled by default.
inventory	Inventory TLVs This TLV is enabled by default.
location	Location Identification TLV This TLV is enabled by default.
network-policy	Network Policy TLV This TLV is enabled by default.

## Disable LLDP Features on the Port

### About this task

Use this procedure to disable LLDP features on the port.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:

```
no lldp [port <portlist>] [status] [config-notification]
```
3. Press Enter.

## Disable LLDP MED Policies for Switch Ports

### About this task

Use this procedure to disable LLDP MED policies for switch ports.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:

```
no lldp med-network-policies [port <portList>] {voice|voice-signaling}
```
3. Press Enter.

## Variable definitions

The following table describes the variables for the `no lldp med-network-policies` command.

Variable	Description
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.

## Disable the Optional Management TLVs

### About this task

Use this procedure to disable the optional Management TLVs so that these TLVs are not included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
no lldp tx-tlv port <portlist> local-mgmt-addr port-desc sys-cap
sys-desc sys-name
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `no lldp tx-tlv` command.

Variables	Description
port <portlist>	The ports affected by the command.
port-desc	The port description TLV. This TLV is enabled by default.
sys-name	The system name TLV. This TLV is enabled by default.
sys-desc	The system description TLV. This TLV is enabled by default.
sys-cap	The system capabilities TLV (default value is false: not included).
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.

## Disable the Optional IEEE 802.1 TLVs

### About this task

Use this procedure to disable the optional IEEE 802.1 TLVs so that these TLVs are not included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable  
configure terminal  
interface Ethernet <port>
```

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

```
no lldp tx-tlv [port <portlist>] dot1 [port-vlan-id] [vlan-name]  
[port-protocol-vlan-id] [protocol-identity [EAP] [LLDP] [STP] ]
```

3. Press Enter.

## Disable the Optional IEEE 802.3 TLVs

### About this task

Use this procedure to disable the optional IEEE 802.3 TLVs so that these TLVs are not included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable  
configure terminal  
interface Ethernet <port>
```

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

```
no lldp tx-tlv port <portlist> dot3 link-aggregation mac-phy-config-  
status maximum-frame-size mdi-power-support
```

3. Press Enter.

## Disable the Optional LLDP MED TLVs

### About this task

Use this procedure to disable the optional LLDP MED TLVs so that these TLVs are not included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
```

```
configure terminal
interface Ethernet <port>
```

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

```
no lldp tx-tlv port <portlist> med extendedPSE inventory location
med-capabilities network-policy
```

3. Press Enter.

## View the LLDP Parameters

### About this task

Use this procedure to display the LLDP parameters.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show lldp [local-sys-data {dot1 | dot3 | med}][med-network-policies
[voice | voice-signaling] [mgmt-sys-data][neighbor {dot1 [vlan-names
| protocol-id]} | [dot3] [detail] | med [capabilities | extended-
power | inventory | location | network-policy] vendor-specific
[call-server [fa-zero-touch] | dot1q-framing | fabric-attach | file-
server | phone-ip | poe-conservation]][neighbor-mgmt-addr] [pdu-tlv-
size][rx-stats ][stats][tx-stats ][tx-tlv [dot1 | dot3 | med |
vendor-specific] [vendor-specific {call-server | dot1q-framing |
file-server | poe-conservation-request-level}]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `show lldp` command.

Variables	Description
local-sys-data {dot1   dot3   med}	<p>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 all med 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>
med-network-policies [voice   voice-signaling]	<p>Displays Media Endpoint Devices (MED) network policies:</p> <ul style="list-style-type: none"> <li>• voice: Displays Voice Network Policies</li> </ul>

*Table continues...*

Variables	Description
	<ul style="list-style-type: none"> <li>• voice-signaling: Displays Voice Signaling Network Policies</li> </ul>
mgmt-sys-data	The local management system data.
<pre>neighbor { dot1 [vlan-names   protocol-id] }   [dot3] [detail]   med [capabilities   extended-power   inventory   location   network-policy] vendor-specific [call-server [fa-zero- touch]   dot1q-framing   fabric-attach   file-server   phone-ip   poe- conservation ]</pre>	<p>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>• detail: displays all TLVs</li> <li>• med: displays MED TLVs</li> <li>• capabilities: Displays Capabilities TLVs</li> <li>• extended-power: Displays extended power TLV</li> <li>• inventory: Displays Inventory TLVs</li> <li>• location: Displays Location TLV</li> <li>• network-policy: Displays Network Policy TLV</li> <li>• vendor-specific: Displays vendor-specific TLVs <ul style="list-style-type: none"> <li>- call-server: Displays neighbors call-server information</li> <li>- fa-zero-touch: Displays neighbors Fabric Attach Zero Touch information</li> <li>- dot1q-framing: Displays neighbors dot1q-framing information</li> <li>- fabric-attach: Displays neighbors Fabric Attach information</li> <li>- file-server: Display neighbors file-server information</li> <li>- phone-ip: Displays neighbors phone-ip information</li> <li>- poe-conservation: Displays neighbors poe-conservation information</li> </ul> </li> </ul>
neighbor-mgmt-addr	Display 802.1ab neighbors management addresses.
pdu-tlv-size	The different TLV sizes and the number of TLVs in an LLDPDU.
port	Port list.
rx-stats	The LLDP receive statistics for the local system.
stats	The LLDP table statistics for the remote system.
tx-stats	The LLDP transmit statistics for the local system.
tx-tlv {dot1   dot3   med}	<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>

*Table continues...*



Variables	Description
	To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.
vendor-specific {call-server   dot1q-framing   file-server   poe-conservation-request-level}	Displays 802.1ab vendor-specific settings: <ul style="list-style-type: none"> <li>• call-server: Displays call-server addresses</li> <li>• dot1q-framing: Displays 802.1Q framing tagging-mode</li> <li>• file-server: Displays file-server addresses</li> <li>• poe-conservation-request-level: Displays PoE conservation request level</li> </ul>

### Sample output: show lldp mgmt-sys-data command

Following is the sample output for the `show lldp` command with the `mgmt-sys-data` variable.

```
Switch>show lldp mgmt-sys-data
```

```
-----
          LLDP mgmt-sys-data
=====
ManagementAddr      MgmtIfId      ManagedEntityOID
-----
IPv4 192.1.1.1      0      1.3.6.4.1.45.3.78.1
-----
```

## View the LLDP Port Parameters

### About this task

Use this procedure to display the LLDP port parameters.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 |
detail | med }][rx-stats] [tx-stats] [pdu-tlv-size] [tx-tlv {dot1 |
dot3 | med | vendor-specific}] [neighbor-mgmt-addr] [neighbor {dot1
| dot3 | detail | med}]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `show lldp port` command.

Variables	Description
local-sys-data {dot1   dot3   detail   med }	The organizationally-specific TLV properties on the local switch: <ul style="list-style-type: none"> <li>• dot1: displays the 802.1 TLV properties</li> <li>• dot3: displays the 802.3 TLV properties</li> </ul>

*Table continues...*

Variables	Description
	<ul style="list-style-type: none"> <li>• detail: displays all organizationally specific TLV properties</li> <li>• med: displays all med 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>
rx-stats	The LLDP receive statistics for the local port.
tx-stats	The LLDP transmit statistics for the local port.
pdu-tlv-size	The different TLV sizes and the number of TLVs in an LLDPDU.
port <portlist>   all	Specifies an individual port, a list of specific ports, or all ports on the switch.
tx-tlv {dot1   dot3   med   vendor-specific}	<p>Display 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> <li>• vendor-specific: displays vendor specific TLV information</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   dot3   detail   med }	<p>The port neighbor TLVs:</p> <ul style="list-style-type: none"> <li>• dot1: displays 802.1 TLVs:</li> <li>• dot3: displays 802.3 TLVs</li> <li>• detail: displays all TLVs.</li> <li>• med: displays MED TLVs</li> <li>• vendor-specific: displays vendor specific TLV information</li> </ul>
[neighbor-mgmt-addr]	<p>The port neighbor LLDP management address.</p> <p>The switch supports IPv4 and IPv6 management addresses.</p>

**Sample: show lldp port command output**

The following is the sample output for **show lldp port** command with the *tx-tlv* variable.

```
Switch(config)#show lldp port 1-5 tx-tlv
-----
LLDP port tlvs
-----
Port  PortDesc  SysName  SysDesc  SysCap  MgmtAddr
-----
1      true       true     true     true     true
2      true       true     true     true     true
3      true       true     true     true     true
4      true       true     true     true     true
5      true       true     true     true     true
-----
```

The following is the sample output for **show lldp port** command with the *local-sys-data dot3* variable.

```
Switch(config)#show lldp port 9 local-sys-data dot3
-----
LLDP local-sys-data chassis
-----
ChassisId:  MAC address          70:7c:69:05:57:00
SysName:
SysCap:    rB / B                (Supported/Enabled)
SysDescr:
Ethernet Routing Switch 5928MTS-uPWR      HW:R0B.1    FW:7.4.0.1b  SW:v7.4.0.053
-----
LLDP local-sys-data port
-----
Port: 9
Dot3-MAC/PHY Auto-neg: supported/enabled      OperMAUtype: 2500BaseTFD
PSE MDI power:      supported/enabled          Port class: PSE
PSE power pair:     spare/not controllable     Power class: 0
  PSE: Type: Type 2 PSE      Source: Primary      Priority: Low
  PSE: PD requested power:   0.0 Watts
  PSE: PSE allocated power:  0.0 Watts
LinkAggr: not aggregatable/not aggregated     AggrPortID: 0
                                                MaxFrameSize: 9216
PMD auto-neg:      100Base(TXFD), (FdxA) Pause, 1000Base(TFD)
-----
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Switch(config)#
```

The following is the sample output for **show lldp port** command with the *neighbor dot3* variable.

```
Switch(config)# show lldp port 7 neighbor dot3
-----
LLDP neighbor
-----
Port: 7      Index: 3                Time: 0 days, 03:31:38
ChassisId:  Network address          IPv4  10.100.41.101
PortId:     MAC address              00:0a:e4:0c:05:ac
SysCap:     TB / TB                  (Supported/Enabled)
PortDesc:   IP Phone
SysDescr:   IP Telephone 2002, Firmware:0604DAD

Dot3-MAC/PHY Auto-neg: supported/enabled      OperMAUtype: 100BaseTXFD
PSE MDI power:      not supported/disabled     Port class: PD
PSE power pair:     signal/not controllable    Power class: 1
PoE+ Power type: Type 2 PD
PoE+ Power priority: High
PoE+ PD requested power: 26.2w
PoE+ PSE allocated power: 26.2w
LinkAggr: not aggregatable/not aggregated     AggrPortID: 0
                                                MaxFrameSize: 1522
PMD auto-neg:      10Base(T, TFD), 100Base(TX, TXFD)
-----
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 2
```

## View the LLDP MED Policy Information

### About this task

Use this procedure to display the LLDP MED policy information for switch ports.

Default med-network-policy for voice have Layer 2 priority 6, DSCP 46, tagging parameter set to untagged and vlan ID 0.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```


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

```
show lldp med-network-policies [port <portList>] {voice|voice-  
signaling}
```

3. Press Enter.

### Variable Definitions

The following table describes the variables for the `show lldp med-network-policies` command.

Variable	Value
port <portlist>	Specifies the port or ports for which to display LLDP MED policy information.
voice	Displays the voice network policy for which to display information. The default value is 46.
voice-signaling	Specifies the voice signalling network policy to disable.
 <b>Note:</b> The default DSCP value is 46 and the default priority value is 6.	

## Configure the PoE Conservation Level Request TLV

### About this task

Use this procedure to request a specific power conservation level for an IP Phone connected to a switch port.

#### Important:

Only Ethernet ports on switches that support PoE can request a specific power conservation level for an IP Phone.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port>
```

- At the command prompt, enter the following command to configure PoE conservation level TLVs for connected IP Phones:

```
lldp [port <portlist>] vendor-specific poe-conservation-request-  
level <0-255>
```

- Set PoE conservation level TLVs for connected IP Phones to the default value by using the following command:

```
default lldp port <portlist> vendor-specific poe-conservation-  
request-level
```

## Variable definitions

The following table describes the variables for the `lldp` command.

Variable	Description
<0-255>	Specifies the power conservation level to request for a vendor specific PD. Values range from 0 to 255. With the default value of 0, the switch does not request a power conservation level for an IP phone connected to the port.
<portList>	Specifies a port or list of ports.

## View the Switch PoE Conservation Level Request TLV Configuration

### About this task

Display PoE conservation level request configuration for local switch ports.

### Procedure

- Enter Privileged EXEC mode:
- Display the PoE conservation level request configuration for one or more switch ports:

```
show lldp [port <portlist>] vendor-specific poe-conservation-  
request-level
```

- Press Enter.

### Example

```
Switch>enable
Switch#configure terminal
Switch(config-if)#vendor-specific poe-conservation-request-level
-----
LLDP vendor-specific POE Request Conservation Level
-----
-----
Unit/      POE Request
Port       Level
-----
1          0
2          0
```

## Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## View PoE Conservation Level Support TLV Information

### About this task

Use this procedure to display PoE conservation level information received on switch ports from an IP phone. To delete all call-server ip addresses configured on DUT, use `default lldp vendor-specific call-server`.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command to view the received PoE conservation level information for one or more switch ports:

```
show lldp [port <portlist>] neighbor vendor-specific poe-
conservation
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## Configure the Switch Call Server IP Address TLV

### About this task

Use this procedure to define the local call server IP addresses that switch ports advertise to Ip Phones. You can define IP addresses for a maximum of 8 local call servers.

### Important:

The switch does not support the advertisement of IPv6 addresses to Ip Phones.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command to define the local call server IPv4 addresses the switch advertises to Ip Phones:

```
lldp vendor-specific call-server [<1-8>] <A.B.C.D> [[<1-8>]
<A.B.C.D>] [[<1-8>] <A.B.C.D>]
```

3. Enter the following command to delete call server IPv4 addresses configured on the switch:

```
default lldp vendor-specific call-server <1-8>
```

## Variable Definitions

The following table describes the variables for the `lldp vendor-specific call-server` command.

Variable	Description
<1-8>	Specifies the call server number.  * <b>Note:</b> When you advertise the IPv4 address of call server 1 only, you do not have to enter a call server number before you enter the IP address.
<A.B.C.D>	Specifies the call server IPv4 address.

## View the Switch Call Server IP Address TLV Configuration

Use this procedure to display information about the defined local call server IP address that switch ports advertise to connected IP phones.

The switch supports a maximum of 8 local call servers.

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command to display call server TLV configuration information for the local switch:  
`show lldp vendor-specific call-server`
3. Press Enter.

### Example

```
Switch>enable
Switch#show lld vendor-specific call-server
-----
                        LLDP Vendor Specific Call Servers IP addresses
-----
Configured Call Server 1: 192.0.1.1
Configured Call Server 2: 192.0.1.2
Configured Call Server 3: 192.0.2.3
-----
```

## View IP Phone Call Server IP Address TLV Information

### About this task

Use this procedure to display call server IP address information received on switch ports from an IP phone.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command to display call server TLV configuration information received on specific switch ports from connected IP phones:

```
show lldp [port <portlist>] neighbor vendor-specific call-server
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## Configure the Switch File Server IP Address TLV

### About this task

Use this procedure to define the local file server IP addresses that switch ports advertise to IP phones. You can define IP addresses for a maximum of 4 local file servers.

#### Note:

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

#### Important:

The switch does not support the advertisement of IPv6 addresses to IP phones.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command to enable file server IPv4 address advertisement to IP phones:

```
lldp vendor-specific file-server [<1-4>] <A.B.C.D> [[<1-4>]
<A.B.C.D>] [[<1-4>] <A.B.C.D>]
```



- To delete file server IPv4 addresses configured on the switch:

```
default lldp vendor-specific file-server <1-4>
```

**\* Note:**

To delete all file-server ip addresses configured on DUT, use `default lldp vendor-specific file-server` command.

## Variable Definitions

The following table describes the variables for the `lldp vendor-specific file-server` command.

Variable	Description
<1-4>	Specifies the file server number.  <b>* Note:</b> When you advertise the IPv4 address of file server 1 only, you do not have to enter a file server number before you enter the IP address.
<A.B.C.D>	Specifies the file server IPv4 address.

## View the Switch File Server IP Address TLV Configuration

Use this procedure to display information about the defined local file server IP address that switch ports advertise to connected IP phones.

You can define IP addresses for a maximum of 4 local file servers.

**! Important:**

The switch does not support the advertisement of IPv6 addresses to IP phones.

### Procedure

- Enter Privileged EXEC mode:  
`enable`
- At the command prompt, enter the following command to display file server TLV configuration information for the switch:  
`show lldp vendor-specific file-server`
- Press Enter.

### Sample: show lldp vendor-specific file-server command output

The following figure displays sample output for the `show lldp vendor-specific file-server` command.

```
Switch>enable
Switch#show lld vendor-specific file-server
-----
LLDP Vendor Specific File Servers IP addresses
-----
Configured Call Server 1: 192.0.1.1
```

```
Configured Call Server 2: 192.0.1.2
Configured Call Server 3: 192.0.2.3
-----
```

## View IP Phone File Server IP Address TLV Information

### About this task

Use this procedure to display information about file server IP address received on switch ports from IP phones.

### Procedure

1. Enter Privileged EXEC mode:
 

```
enable
```
2. At the command prompt, enter the following command to display file server advertisement configuration information received on specific switch ports from connected IP phones:
 

```
show lldp [port <portlist>] neighbor vendor-specific file-server
```
3. Press Enter.

### Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## Configure the 802.1Q Framing TLV

### Before you begin

- Enable LLDP MED capabilities.
- Enable LLDP MED network policies.

### About this task

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an IP phone.

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable

configure terminal

interface Ethernet <port>
```
2. At the command prompt, enter the following command to configure the Layer 2 frame tagging mode:
 

```
lldp [port <portlist>] vendor-specific dot1q-framing [tagged | non-
tagged | auto]
```

3. Enter the following command to set the Layer 2 frame tagging mode to default:

```
default lldp [port <portlist>] vendor-specific dot1q-framing
```

## Variable definitions

The following table describes the variables for the `lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.
[tagged   non-tagged   auto]	<p>Specifies the frame tagging mode. Values include:</p> <ul style="list-style-type: none"> <li>• <b>tagged</b>—frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV.</li> <li>• <b>non-tagged</b>—frames are not tagged with 802.1Q priority.</li> <li>• <b>auto</b>—an attempt is made to tag frames based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged.</li> </ul> <p>The default tagging mode is auto.</p>

## View the Switch 802.1Q Framing TLV Configuration

### About this task

Display the configured Layer 2 frame tagging mode for switch ports.

### Procedure

1. Enter Privileged EXEC mode:
 

```
enable
```
2. Display the configured Layer 2 frame tagging mode for one or more switch ports:
 

```
show lldp [port <portlist>] vendor-specific dot1q-framing
```
3. Press Enter.

### Example

```
Switch(config)#interface fastethernet 1-10
Switch(config-if)#show lldp vendor-specific dot1q-framing
```

```
-----
LLDP vendor-specific 802.1Q Framing
-----
-----
```

Unit/ Port	Framing Tagging Mode
1	tagged
2	auto

```
-----
```

```

3          auto
4          auto
5          auto
6          auto
7          auto
8          auto
9          auto
10         auto

```

### Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## View IP phone 802.1Q Framing TLV Information

### About this task

Use this procedure to display Layer 2 frame tagging mode information received on switch ports from connected IP phones.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command to display the received Layer 2 frame tagging mode information for one or more switch ports:

```
show lldp [port <portlist>] neighbor vendor-specific dot1q-framing
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## Configure TLV Transmission Flags

### About this task

Use this procedure to configure the transmission of optional proprietary TLVs from switch ports to IP phones.

#### Note:

The switch transmits configured TLVs only on ports with the TLV transmit flag enabled.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

2. To select the TLVs that the switch transmits, enter the following command:

```
lldp tx-tlv [port <portList>] vendor-specific {[call-server] [dot1q-
framing] [file-server] [poe-conservation]}
```

3. To disable the transmission of optional proprietary TLVs, enter the following command:

```
no lldp tx-tlv [port <portList>] vendor-specific {[call-server]
[dot1q-framing] [file-server] [poe-conservation] }
```

4. To restore TLVs transmission to default, enter the following command:

```
default lldp tx-tlv [port <portList>] vendor-specific {[call-server]
[dot1q-framing] [file-server] [poe-conservation]}
```

## Variable Definitions

The following table describes the parameters for the `lldp tx-tlv` command.

Variable	Value
call-server	Sets the call server TLV transmit flag state. The default state is enabled
dot1q-framing	Sets the Layer 2 priority tagging TLV transmit flag state. The default state is enabled.
file-server	Sets the file server TLV transmit flag state. The default state is enabled.
poe-conservation	Sets the PoE conservation request TLV transmit flag state. The default state is enabled.
<portList>	Specifies a port or list of ports.

## Display TLV Transmit Flag Status

### About this task

Use this procedure to display the status of transmit flags for switch ports on which IP phone support TLVs are configured.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
show lldp [port <portlist>] tx-tlv vendor-specific
```

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `show lldp` command.

Variable	Definition
<portlist>	Specifies a port or list of ports.

## Display IP Phone IP TLV Configuration

### About this task

Use this procedure to display IP address configuration information received on switch ports from connected IP phones.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show lldp [port <portlist>] neighbor vendor-specific phone-ip
```

3. Press Enter.

### Variable definitions

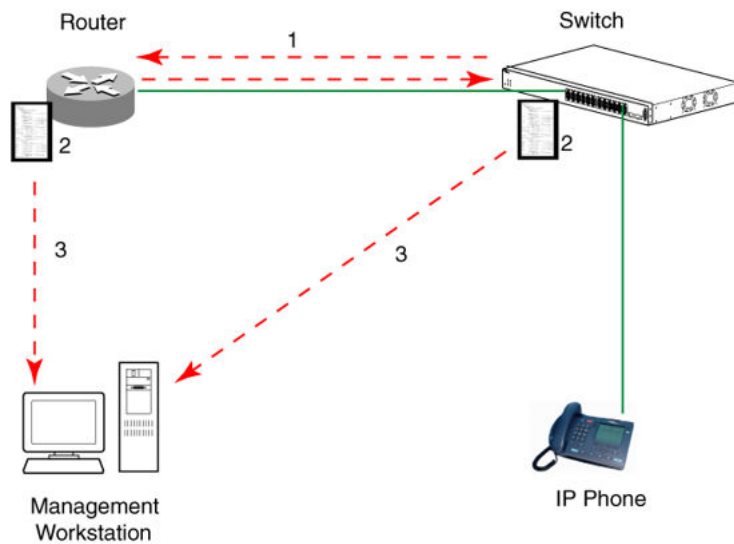
Use the data in the following table to use the `show lldp` command.

Variable	Definition
<portlist>	Specifies a port or list of ports.

## LLDP Configuration Example

By default, LLDP is enabled for Tx and Rx on all switch ports. The default value for the LLDP Tx interval is 30 seconds (LLDPDUs are sent at 30 seconds). With the default settings, only the default enabled for transmission TLVs are sent, but the switch can receive any LLDP Core, DOT1, DOT3 TLV, or Med-capabilities TLV from its peers.

The following figure shows an example of LLDP configuration. For this example, the router is connected to the switch port 1 and the IP Phone uses port 13.



**Figure 10: LLDP configuration example**

To configure the example shown in the preceding figure, you must perform the following tasks:

1. Modify the default LLDP Tx interval from (the default 30 second value) to 60 seconds.  
Note that if any modification is detected in the LLDP local-sys-data before the Tx interval expires, an LLDPDU is immediately sent on all active links to update the peers neighbor tables.
2. Enable the Port Description TLV for transmission. (contains the description of the 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 can be handled by the LLDP sending port)
15. Enable the Location Identification TLV for transmission. (indicates the physical location of the LLDP sending port; three coordinate sets are available to configure and send)
16. Enable the Extended Power-via-MDI TLV for transmission. (provides detailed informations regarding the PoE parameters of the LLDP sending device)
17. Enable the Inventory – Hardware Revision TLV for transmission. (indicates the hardware revision of the LLDP sending device)
18. Enable the Inventory – Firmware Revision TLV for transmission. (indicates the firmware revision of the LLDP sending device)
19. Enable the Inventory – Software Revision TLV for transmission. (indicates the software revision of the LLDP sending device)
20. Enable the Inventory – Serial Number TLV for transmission. (indicates the serial number of the LLDP sending device)
21. Enable the Inventory – Manufacturer Name TLV for transmission. (indicates the manufacturer name of the LLDP sending device)
22. Enable the Inventory – Model Name TLV for transmission. (indicates the model name of the LLDP sending device)
23. Configure the location information for the LLDP-MED Location Identification TLV. (There are three coordinate sets available for location advertisement.)
24. Enable the LLDP-MED Capabilities TLV for transmission (indicates the supported LLDP-MED TLVs and the LLDP-MED device type of the LLDP sending device)

## Detailed Configuration Commands

The following section describes the detailed CLI commands required to carry out the configuration depicted by [Figure 10: LLDP configuration example](#) on page 223.

### Modify the default LLDP Tx interval:

```
Switch>enable
Switch#configure terminal
Switch(config)#lldp tx-interval 60
```

### Check the new LLDP global settings:

```
Switch(config)# show lldp

802.1ab configuration:
-----
TxInterval:60
TxHoldMultiplier:4
RxInitDelay:2
TxDelay:2
```



```
NotificationInterval:5
MedFastStartRepeatCount:4
```

### Enable all LLDP Core TLVs for transmission on the router and IP Phone ports:

```
Switch(config)#interface Ethernet 1/13
Switch(config-if)#lldp tx-tlv port 1/13 port-desc
Switch(config-if)#lldp tx-tlv port 1/13 sys-name
Switch(config-if)#lldp tx-tlv port 1/13 sys-desc
Switch(config-if)#lldp tx-tlv port 1/13 sys-cap
Switch(config-if)#lldp tx-tlv port 1/13 local-mgmt-addr
```

### Check the LLDP settings of the router and IP Phone ports:

```
Switch(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
-----
```

### Enable all LLDP DOT1 TLVs for transmission on the router and IP Phone ports:

```
Switch(config-if)#lldp tx-tlv port 1/13 dot1 port-vlan-id
Switch(config-if)#lldp tx-tlv port 1/13 dot1 port-protocol-vlan-id
Switch(config-if)#lldp tx-tlv port 1/13 dot1 vlan-name
Switch(config-if)#lldp tx-tlv port 1/13 dot1 protocol-identity EAP LLDP STP
```

### Check the LLDP settings of the router and IP Phone ports:

```
Switch(config-if)# show lldp port 1/13 tx-tlv dot1
```

```
-----
                        LLDP port dot1 tlvs
-----
Dot1 protocols: STP,EAP,LLDP
-----
Port  PortVlanId  VlanNameList          PortProtocolVlanId  ProtocolIdentity
-----
13    true        1,3,5,7,9,117-118    1,3,5,7,9,117-118  EAP,LLDP
-----
```

### Enable all LLDP DOT3 TLVs for transmission on the router and IP Phone ports:

```
Switch(config-if)#lldp tx-tlv port 1/13 dot3 mac-phy-config-status
Switch(config-if)#lldp tx-tlv port 1/13 dot3 mdi-power-support
Switch(config-if)#lldp tx-tlv port 1/13 dot3 link-aggregation
Switch(config-if)#lldp tx-tlv port 1/13 dot3 maximum-frame-size
```

### Check the LLDP settings of the router and IP Phone ports:

```
Switch(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
13    true        true          true          true
-----
```

## Enable all LLDP MED TLVs for transmission on the router and IP Phone ports:

The first three commands are required to configure the location identification for the LLDP-MED Location Identification TLV.

```
Switch(config-if)#lldp location-identification civic-address country-code US city Boston
street Orlando
Switch(config-if)#lldp location-identification coordinate-base altitude 234 meters datum
WGS84
Switch(config-if)#lldp location-identification ecs-elin 1234567890
Switch(config-if)#lldp tx-tlv port 1/12-13 med med-capabilities
Switch(config-if)#lldp tx-tlv port 1/12-13 med network-policy
Switch(config-if)#lldp tx-tlv port 1/12-13 med location
Switch(config-if)#lldp tx-tlv port 1/12-13 med extendedPSE
Switch(config-if)#lldp tx-tlv port 1/12-13 med inventory
```

## Check the new LLDP settings of the router and IP Phone ports:

```
Switch(config-if)#show lldp tx-tlv med
```

```
-----
LLDP port med tlvs
-----
Port Med      Network  Location  Extended  Inventory
  Capabilities Policy          PSE
-----
12   true     true     true     true     true
13   true     true     true     true     true
-----
```

MED TLVs are transmitted only if Med-Capabilities TLV is transmitted

## Enable all the LLDP Vendor Specific TLVs for transmission on the IP Phone ports:

```
Switch(config-if)#lldp tx-tlv port 1/13 vendor-specific call-server
Switch(config-if)#lldp tx-tlv port 1/13 vendor-specific dot1q-framing
Switch(config-if)#lldp tx-tlv port 1/13 vendor-specific file-server
Switch(config-if)#lldp tx-tlv port 1/13 vendor-specific poe-conservation
```

## Check the LLDP settings of the IP Phone port:

```
Switch(config-if)#show lldp port 1/13 tx-tlv vendor-specific
```

```
-----
LLDP port Vendor-Specific TLVs
-----
Unit/ POE Conservation  Call  File  Dot1Q  FA Element  FA I-SID/
Port  Request          Server Server Framing  Type      VLAN Asgns
-----
13    true             true  true  true   n/a         n/a
```

---

## Configuring Asset ID String

Use the information in this section to configure an asset ID for the switch or stack.

### Configure the Asset ID String

#### About this task

Use this procedure to configure the Asset ID of a switch or stack.

**Procedure**

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. At the command prompt, enter the following command:  

```
asset-id [stack|unit <1-8>] <WORD>
```
3. Press Enter.

**Next steps**

Use the following commands to view the configured Asset ID:

- `show system`
- `show sys-info`
- `show tech`
- `show system verbose`

**Variable definitions**

Use the data in the following table to use the `asset-id` command.

Variable	Definition
<code>stack</code>	Sets the Asset ID of the stack.
<code>unit &lt;1-8&gt;</code>	Sets the Asset ID of a specific unit.
<code>&lt;WORD&gt;</code>	Sets the Asset ID of the unit on which it is the console.

**Disable the Asset ID String****About this task**

Use this procedure to disable the asset ID string.

**Procedure**

1. Enter Global Configuration mode:  

```
enable
configure terminal
```
2. At the command prompt, enter the following command:  

```
no asset-id [stack | unit <1-8>]
```
3. Press Enter.

**Next steps**

Use the `show system` command to verify the Asset ID sting settings.

## Variable definitions

Use the data in the following table to use the `no asset-id` command.

Variable	Definition
stack	Sets the Asset ID of the stack.
unit <1-8>	Specifies the Asset ID for specified unit in the stack.

## Restore the default Asset ID String

### About this task

Use this procedure to set the asset ID string to default mode.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
default asset-id [stack | unit <1-8>]
```
3. Press Enter.

### Next steps

Use the `show system` command to verify the Asset ID string settings.

## Variable definitions

Use the data in the following table to use the `default asset-id` command.

Variable	Definition
stack	Sets the default Asset ID of the stack.
unit <1-8>	Specifies the default Asset ID for specified unit.

---

## Configuring Energy Saver

With Extreme Networks Energy Saver, you can configure the switch to utilize energy more efficiently.

Use the information in this section to configure Energy Saver.

### Configure Global Energy Saver

#### About this task

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

## Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```





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

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

3. Press Enter.

## Variable Definitions

Use the data in the following table to use the `energy-saver` command.

Variable	Definition
[default]	Configures Energy Saver efficiency mode, POE power saving, or global Energy Saver to default values (disabled).
efficiency-mode	<p>Enables Energy Saver efficiency mode.</p> <ul style="list-style-type: none"> <li> <b>Note:</b> You must ensure that SNTP is enabled before you can enable Energy Saver efficiency mode.</li> <li> <b>Note:</b> You must disable Energy Saver globally before you can modify Energy Saver efficiency mode.</li> <li> <b>Note:</b> When enabled, Energy Saver efficiency mode overrides custom Energy Saver scheduling and PoE power saving mode. You will be prompted to confirm that you want to enable Energy Saver efficiency mode before proceeding.</li> </ul>
enable	Enables Energy Saver globally.
[no]	Disables Energy Saver efficiency mode, POE power saving, or Energy Saver globally.
poe-power-saving	<p>Enables POE power saving.</p> <ul style="list-style-type: none"> <li> <b>Note:</b> You must disable Energy Saver globally before you can modify POE power saving.</li> </ul>

## Configure Port-based Energy Saver

### Before you begin

Disable Energy Saver globally.

**About this task**

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

**Procedure**

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

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

3. Press Enter.

**Variable definitions**

Use the data in the following table to use the `[default] [no] energy-saver` command.

Variable	Definition
<enable>	Enables Energy Saver for the accessed port.
[no]	Disables Energy Saver for the accessed port, an alternate port, or list of ports.
port <portlist> enable	Enables Energy Saver for a port or list of ports.

**Activate or Deactivate Energy Saver Manually****Before you begin**

Disable Energy Saver globally.

**About this task**

Activate Energy Saver to ensure that Energy Saver is enabled and activated.

**Procedure**

1. Enter Privileged EXEC mode:

```
enable
```

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

```
energy-saver {activate | deactivate}
```

3. Press Enter.

**Configure Energy Saver Scheduling****Before you begin**

Disable Energy Saver globally.

## About this task

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.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
energy-saver schedule {weekday|weekend|monday|tuesday|wednesday|
thursday|friday|saturday|sunday} <hh:mm> {activate|deactivate}
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `energy-saver schedule {weekday|weekend|monday|tuesday|wednesday|thursday|friday|saturday|sunday} <hh:mm> {activate|deactivate}` command.

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

## Disable Energy Saver Scheduling

### Before you begin

Disable Energy Saver globally.

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
no energy-saver schedule
```

3. Press Enter.

### Variable definitions

The following table defines optional parameters that you can enter after the `no energy-saver schedule` command.

Variable	Description
<code>friday monday saturday sunday thursday tuesday wednesday</code>	Disables Energy Saver scheduling for a specific day.
<code>weekday</code>	Disables Energy Saver scheduling for all weekdays.
<code>weekend</code>	Disables Energy Saver scheduling for Saturday and Sunday.
<code>&lt;hh:mm&gt;</code>	Specifies the scheduled Energy Saver start time (hour and minutes).

## Configure Energy Saver Scheduling to Default

### Before you begin

Disable Energy Saver globally.

### About this task

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

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

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

```
default energy-saver schedule
```

3. Press Enter.

### Variable definitions

The following table defines optional parameters that you can enter after the `default energy-saver schedule` command.



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

## View Energy Saver Scheduling

### About this task

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

### Procedure

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

```
show energy-saver schedule
```
3. Press Enter.

### Example

```
Switch#show energy-saver schedule
Day      Time  Action
-----  ----  -
Monday   08:00  Activate
Wednesday 11:00  Activate
Friday   14:00  Activate
```

## View Energy Saver Savings

### About this task

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

### Procedure

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

```
show energy-saver savings
```
3. Press Enter.

#### 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.

### Example

```
Switch#show energy-saver savings
Unit# Model          Switch Capacity Saving PoE Saving
-----
1    <Switch#>        0.0 watts              N/A
-----
TOTAL                0.0 watts              0.0 watts
=====
```

## View the Global Energy Saver Configuration

### About this task

Use the following procedure to review the Energy Saver configuration for the switch.

### Procedure

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

```
show energy-saver
```

3. Press Enter.

### Example

```
Switch#show energy-saver
Extreme Energy Saver (Energy Saver):Disabled
Energy Saver PoE Power Saving Mode: Disabled
Energy Saver Efficiency-Mode Mode: Disabled
Day/Time: Not set
Current Energy Saver state: Energy Saver is Inactive
```

## View Port-based Energy Saver Configuration

### About this task

Use the following procedure to review Energy Saver configuration for all ports on the switch, an individual port, or range of ports.

### Procedure

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

```
show energy-saver interface <portlist>
```

3. Press Enter.

### Example

```
Switch#show energy-saver interface 1-6
Port    AES State PoE Savings PoE Priority
-----
1       Disabled N/A         N/A*
2       Disabled N/A         N/A*
3       Disabled N/A         N/A*
```

4	Disabled	N/A	N/A*
5	Disabled	N/A	N/A*
6	Disabled	N/A	N/A*

## Variable definitions

The following table defines optional parameters that you can enter after the `show energy-saver interface` command.

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

## Enable or Disable UTC Timestamp in CLI show command Outputs

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

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To enable the display of the UTC timestamp, enter the following command:

```
cli timestamp enable
```

3. To disable the display of the UTC timestamp, enter the following command:

```
no cli timestamp enable
```

## Enable the Web Server for EDM

You must enable the Web server before you can start Enterprise Device Manager. For information about enabling the Web server using CLI, see [Using CLI and EDM on Ethernet Routing Switch 4900 and 5900 Series](#).

## Configure the EDM Inactivity Time Out using CLI

By default, a session becomes inactive if there is no interaction with the EDM interface for more than 15 minutes. You can configure the time period for which an EDM session remains active.

### edm inactivity-timeout

The `edm inactivity-timeout` command enables the EDM inactivity time out period.

Following is the syntax for this command:

```
edm inactivity-timeout <30-65535>
```

Run `edm inactivity-timeout` command in Global Configuration mode.

### **default edm inactivity-timeout**

The `edm inactivity-timeout` command sets the EDM inactivity time out period to factory default. The default time out period is 15 minutes.

Following is the syntax for this command:

```
default edm inactivity-timeout
```

Run `default edm inactivity-timeout` command in Global Configuration mode.

### **show edm inactivity-timeout**

The `show edm inactivity-timeout` command displays the EDM inactivity time out period settings.

Following is the syntax for this command:

```
show edm inactivity-timeout
```

Run `show edm inactivity-timeout` command in Global Configuration mode.

### **no edm inactivity-timeout**

The `no edm inactivity-timeout` command disables the EDM inactivity time out period settings.

Following is the syntax for this command:

```
no edm inactivity-timeout
```

Run `no edm inactivity-timeout` command in Global Configuration mode.

---

## **Configuring Jumbo Frames**

This section describes the procedures you can perform to configure jumbo frames on a switch or stack using CLI commands.

### **Enable Jumbo Frames**

#### **About this task**

Use the following procedure to enable jumbo frames on a switch or stack:

#### **Procedure**

1. Enter Global Configuration mode:

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:

```
jumbo-frames [enable]
```
3. Press Enter.

## Disable Jumbo Frames

### About this task

Use the following procedure to disable jumbo frames on a switch or stack.

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:  

```
no jumbo-frames [enable]
```
3. Press Enter.

## Configure the Size of Jumbo Frames

### About this task

Use the following procedure to configure the size of jumbo frames on a switch or stack. The default is 9216 bytes.

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:  

```
jumbo-frames size <1519 - 9216>
```
3. To reset the size to the default value, enter the following command:  

```
default jumbo-frames size
```

## Reset the State of Jumbo Frames

### About this task

Use the following procedure to reset the jumbo frames state to default on a switch or stack. The default state is enabled.

### Procedure

1. Enter Global Configuration mode:  

```
enable  
configure terminal
```
2. At the command prompt, enter the following command:  

```
default jumbo-frames [enable]
```

## Display the State of Jumbo Frames

### About this task

Use the following procedure to display the state of jumbo frames and MTU size.

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command:  
`show jumbo-frames`
3. Press Enter.

---

## Configuring System using the EDM

This section provides procedures you can use to configure the switch or stack with Enterprise Device Manager (EDM).

---

## Configure 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, 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**.

## Configure Out-Of-Band Management using EDM

Use this procedure to configure the out-of-band management IP address, subnet mask, and default gateway.

### About this task

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

#### \* Note:

The out-of-band management IP address must be different than the switch or stack in-band management IP address.

### Procedure

1. From the navigation pane, double-click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Switch/Stack**.
4. In the Switch/Stack work area, click the **Management IP** tab.
5. To configure out-of-band management parameters for a switch, double-click table cells as required.
6. On the toolbar, click **Apply**.
7. On the toolbar, you can click **Refresh** to verify the out-of-band management configuration.

## Field Descriptions

The following table describes the fields associated with configuration of an out-of-band management.

Name	Description
<b>Unit</b>	Indicates a stack switch unit, for which to configure an out-of-band management IP address. Values range from 1 to 8.  For a stack environment, a <b>Unit</b> value of 1 specifies the base unit.  For a standalone switch, the <b>Unit</b> value is 1.
<b>IpMgmtAddress</b>	Specifies an out-of-band management IP address for the selected switch.  DEFAULT for IPv4: 0.0.0.0
<b>IpMgmtNetMask</b>	Specifies the subnet mask associated with the out-of-band management IP address.

*Table continues...*

Name	Description
	DEFAULT for IPv4: 0.0.0.0
<b>IpMgmtGateway</b>	<p>Specifies the IP address for the out-of-band management default gateway.</p> <p>DEFAULT for IPv4: 0.0.0.0</p> <p>DEFAULT for IPv6: 0:0:0:0:0:0</p> <p><b>!</b> <b>Important:</b></p> <p>If you configure an out-of-band default gateway, the device disables the in-band default gateway. The out-of-band management default gateway takes precedence over the in-band management default gateway.</p>
<b>Ipv6MgmtAddress</b>	<p>Specifies an out-of-band management IP address for the selected switch.</p> <p>Specifies the IPv6 address associated with the physical dedicated out-of-band management port of a component. For a stackable system in stack mode, this IPv6 address always applies to the individual units in the stack.</p> <p>DEFAULT for IPv6: 0::0/0</p>
<b>Ipv6MgmtNetMask</b>	<p>Specifies the subnet mask associated with the out-of-band management IP address.</p> <p>Specifies the IPv6 address associated with the physical dedicated out-of-band management port of a component. For a stackable system in stack mode, this netmask always applies to the individual units in the stack.</p> <p>DEFAULT for IPv6: 0::0/0</p>
<b>IpMgmtShutdown</b>	<p>Specifies whether to enable or disable the management port for the unit. A value of true disables the port.</p> <p>DEFAULT: false</p>

## Configure 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, 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** .

## Field Descriptions

Use the data in this table to configure remote access for a switch.

Name	Description
Telnet Remote Access Setting	<p>Specifies the remote access settings for telnet sessions.</p> <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	<p>Specifies SNMP remote access settings.</p> <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	<p>Specifies web page remote access settings.</p> <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	<p>Specifies the remote access settings for SSH.</p> <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>

## Configure 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, 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** .

## Field Descriptions

Use the data in this table to configure a list of IPv4 source addresses to permit access to the switch.

Name	Description
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.

---

## Configure 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, 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** .

## Field Descriptions

Use the data in this table to configure a list of IPv6 source addresses for which to permit access to the switch .

Name	Description
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.

## Customizing the EDM Logon Banner

Use the information in this section to customize the EDM logon banner.

### Customize the Logon Banner using EDM

Use this procedure to customize the banner that is displayed on the the EDM logon page.

#### Before you begin

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

#### Procedure

1. In the navigation tree, open the following folders: **Edit > Chassis > Chassis > Custom banner**.
2. In the work area, click the **Custom Banner** tab.
3. Click a row to select the switch for which to customize the banner.
4. In the row, double-click the cell in the **Line** column.
5. Type a character string for the banner.
6. Click **Apply**.

### Field Descriptions

Use the data in the following table to configure the logon banner.

Name	Description
<b>Type</b>	Indicates whether the banner type is for a standalone (switch) or a stack (stack).
<b>Id</b>	Indicates the line of text within a custom banner.
<b>Line</b>	Specifies the banner character string. The custom banner is 19 lines high and can be up to 80 characters long.

## Configure the Logon Banner in EDM

### Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, click the **Banner** tab.
5. In the **BannerControl** section, click desired banner configuration.
6. Click **Apply**.

### Field Descriptions

Use the information in the following table to select the banner type.

Name	Description
BannerControl	<p>Specifies the banner to be displayed as soon as you connect to a switch or stack. Values include:</p> <ul style="list-style-type: none"> <li>• static—uses the predefined static banner.</li> <li>• custom—uses the previously set custom banner.</li> <li>• disabled—prevents the display of any banner.</li> </ul>

---

## Running Script Configuration using EDM

You can use the scripts to configure the parameters for the switch. The scripts can be executed in a default or verbose mode. Run scripts are available in non-verbose and verbose mode for IP Office, and verbose mode for Link Layer Discovery Protocol (LLDP) and Auto Detect Auto Configuration (ADAC).

Use the procedures in this section to configure using IP Office, LLDP, and ADAC scripts.

### Configure IP Office Script using EDM

Use the following procedure to configure IP Office in default or verbose mode using run scripts.

**\* Note:**

This script does not work in an SPBM environment and should only be used when the switch is at default configuration.

**\* Note:**

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

## Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Run Script**.
3. In the work area, click the **IP Office Script** tab.
4. In the Mode work area, from the **Run Script Mode** dialog box, select **default** to execute the script in the default mode or select **verbose** to modify the predefined values.  
If you select **default**, the parameters are automatically configured. If you select **verbose**, proceed with the following steps to modify the parameters in verbose mode.
5. In the Verbose work area, type the Voice VLAN ID in the **Voice VLAN Id** dialog box.
6. In the **Voice VLAN Gateway** dialog box, type the VLAN IP address.
7. In the **Voice VLAN Gateway Mask** dialog box, enter the VLAN IP mask address.
8. In the **Data VLAN Id** dialog box, type the data VLAN ID.
9. In the **Data VLAN Gateway** dialog box, type the data VLAN Gateway IP address.
10. In the **Data VLAN Gateway Mask** dialog box, type the data VLAN Gateway IP mask address.
11. In the **IP Route to Gateway Modem-Router** dialog box, type the IP route address of the Gateway Modem-Router.
12. In the **IP Office Call-Server** dialog box, type the call server IP address.
13. In the **IP Office File-Server** dialog box, type the file server IP address.
14. Click **Apply**.

## Field Descriptions

The following table describes the fields associated with scripts to configure the parameters for the switch.

Name	Description
Run Script Mode	Specifies to run the script either in default or verbose mode.
Voice VLAN ID	Specifies the voice VLAN ID. By default, the voice VLAN ID is 42.
Voice VLAN Gateway	Specifies the Voice VLAN Gateway IP Address. By default, the voice VLAN gateway IP address is 192.168.42.254.
Voice VLAN Gateway Mask	Specifies the voice VLAN gateway IP mask address. By default, the voice VLAN gateway IP mask address is 255.255.255.0.  The default subnet mask created by the run IP Office script supports a maximum of 250 hosts. You can change the subnet mask to 255.255.254.0 to allow 510 hosts for each subnet using the verbose mode.
Data VLAN ID	Specifies the data VLAN ID. By default, the data VLAN ID is 44.

*Table continues...*

Name	Description
Data VLAN Gateway	Specifies the data VLAN Gateway. By default, the data VLAN Gateway is 192.168.44.254.
Data VLAN Gateway Mask	Specifies the data VLAN Gateway Mask. By default, the data VLAN Gateway Mask is 255.255.255.0.
IP Route to Gateway Modem-Router	Specifies the IP Route to gateway modem and router. By default, the IP address is 192.168.44.2.
IP Office Call-Server	Specifies the IP Office call server IP address. By default, the call server IP address is 192.168.42.1.
IP Office File-Server	Specifies the IP Office file server IP address. By default, the file server IP address is 192.168.42.1.
Status	Displays the status of the last action that occurred since the switch last booted. Values include: <ul style="list-style-type: none"> <li>• other—no action occurred since the last boot.</li> <li>• inProgress—the selected operation is in progress.</li> <li>• passed—the selected operation succeeded.</li> <li>• failed—the selected operation failed.</li> </ul>

## Configure ADAC Script using EDM

Use the following procedure to configure ADAC in verbose mode using Run Scripts.

### \* Note:

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

### Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Run Script**.
3. In the work area, click the **ADAC Script** tab.
4. In the Mode work area, by default, **verbose** is selected in the **Run Script Mode** dialog box.
5. **(Optional)** In the Verbose work area, type the data VLAN ID in the **Data VLAN Id** dialog box.
6. Select **Management VLAN flag** if you want the data VLAN as the management VLAN.
7. **(Optional)** In the **Data VLAN Gateway** dialog box, type the data VLAN Gateway IP address. In the **Data VLAN Gateway Mask** dialog box, type the data VLAN Gateway mask address.
8. **(Optional)** In the **Management IP address** dialog box, type the management IP address. In the **Management IP Mask** dialog box, type the management IP mask.
9. In the **Default IP Route** dialog box, type the default IP route address.
10. In the **Voice VLAN Id** dialog box, type the voice VLAN ID.

11. **(Optional)** In the **Voice VLAN Gateway** dialog box, type the IP address. In the **Voice VLAN Gateway Mask** dialog box, type the IP mask address.
12. In the **LLDP Call-Server** dialog box, type the LLDP call server IP address.
13. In the **LLDP File-Server** dialog box, LLDP file server IP address.
14. **(Optional)** Select the **Uplink trunk flag** to link ADAC uplink port as a member of MLT trunk.
15. Click the **ADAC Uplink Ports** ellipsis (...).
16. From the ADAC Uplink Ports, select the uplink ports and then, click Ok.
17. Click the **ADAC Call Server Ports** ellipsis (...).
18. From the ADAC Call Server ports, select the call server ports and then, click Ok.
19. Click the **ADAC Telephony Ports** ellipsis (...).
20. From the ADAC Telephony Ports, select the telephony ports and then, click Ok.
21. Click **Apply**.

## Field Descriptions

The following table describes the fields associated with configuration of ADAC in verbose mode using Run Scripts.

Name	Description
Run Script Mode	Specifies to run the script in verbose mode and it is selected by default.
Data VLAN Id	Specifies the data VLAN ID. The value ranges from 1 to 4096.
Management VLAN flag	Specifies data VLAN ID as Management VLAN. This is optional.
Data VLAN Gateway	Specifies the data VLAN gateway IP address.
Data VLAN Gateway Mask	Specifies the data VLAN gateway mask IP address.
Management IP address	Specifies the management IP address.
Management IP Mask	Specifies the management IP mask address.
Default IP Route	Specifies the default IP route.
Voice VLAN Id	Specifies the voice VLAN ID. By default, the voice VLAN ID is 42.
Voice VLAN Gateway	Specifies the Voice VLAN Gateway IP Address. By default, the voice VLAN gateway IP address is 192.168.42.254.
Voice VLAN Gateway Mask	Specifies the voice VLAN gateway IP mask address. By default, the voice VLAN gateway IP mask address is 255.255.255.0.
LLDP Call-Server	Specifies the LLDP call server IP address.
LLDP File-Server	Specifies the LLDP file server IP address.
Uplink trunk flag	Links the ADAC uplink port to the MLT trunk.
ADAC Uplink Ports	Specifies the ADAC uplink ports. A maximum of 50 ports are supported.

*Table continues...*

Name	Description
ADAC Call Server Ports	Specifies the ADAC call server ports. A maximum of 50 ports are supported.
ADAC Telephony Ports	Specifies the ADAC telephony ports. A maximum of 50 ports are supported.
Status	Displays the status of the last action that occurred since the switch last booted. Values include: <ul style="list-style-type: none"> <li>• other—no action occurred since the last boot.</li> <li>• inProgress—the selected operation is in progress.</li> <li>• passed—the selected operation succeeded.</li> <li>• failed—the selected operation failed.</li> </ul>

## Configure LLDP Script using EDM

Use the following procedure to configure LLDP in verbose mode using Run Scripts.

### Note:

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

### Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Run Script**.
3. In the work area, click the **LLDP Script** tab.
4. In the Mode work area, by default, verbose is selected in the **Run Script Mode** dialog box.
5. **(Optional)** In the Verbose work area, type the data VLAN ID in the **Data VLAN Id** dialog box.
6. Select **Management VLAN flag** if you want the data VLAN as the management VLAN.
7. **(Optional)** In the **Data VLAN Gateway** dialog box, type the data VLAN Gateway IP address. In the **Data VLAN Gateway Mask** dialog box, type the data VLAN Gateway mask address.
8. Click the **Data VLAN Uplink Ports** ellipsis (...).
9. From the Data VLAN Uplink Ports, select the uplink ports and click Ok.
10. **(Optional)** In the **Management IP address** dialog box, type the management IP address. In the **Management IP Mask** dialog box, type the management IP mask.
11. In the **Default IP Route** dialog box, type the default IP route address.
12. In the **Voice VLAN Id** dialog box, type the voice VLAN ID.
13. **(Optional)** In the **Voice VLAN Gateway** dialog box, type the IP address. In the **Voice VLAN Gateway Mask** dialog box, type the IP mask address.
14. In the **LLDP Call-Server** dialog box, type the LLDP call server IP address.



15. In the **LLDP File-Server** dialog box, LLDP file server IP address.
16. Click **Apply**.

## Field Descriptions

The following table describes the fields associated with configuration of LLDP in verbose mode using Run Scripts.

Name	Description
Run Script Mode	Specifies to run the script in verbose mode and it is selected by default.
Data VLAN Id	Specifies the data VLAN ID. The value ranges from 1 to 4096.
Management VLAN flag	Specifies data VLAN ID as Management VLAN. This is optional.
Data VLAN Gateway	Specifies the data VLAN gateway IP address.
Data VLAN Gateway Mask	Specifies the data VLAN gateway mask IP address.
Data VLAN Uplink Ports	Specifies the data VLAN uplink ports.
Management IP address	Specifies the management IP address.
Management IP Mask	Specifies the management IP mask address.
Default IP Route	Specifies the default IP route.
Voice VLAN Id	Specifies the voice VLAN ID. By default, the voice VLAN ID is 42.
Voice VLAN Gateway	Specifies the Voice VLAN Gateway IP Address. By default, the voice VLAN gateway IP address is 192.168.42.254.
Voice VLAN Gateway Mask	Specifies the voice VLAN gateway IP mask address. By default, the voice VLAN gateway IP mask address is 255.255.255.0.
LLDP Call-Server	Specifies the LLDP call server IP address.
LLDP File-Server	Specifies the LLDP file server IP address.
Status	Displays the status of the last action that occurred since the switch last booted. Values include: <ul style="list-style-type: none"> <li>• other—no action occurred since the last boot.</li> <li>• inProgress—the selected operation is in progress.</li> <li>• passed—the selected operation succeeded.</li> <li>• failed—the selected operation failed.</li> </ul>

---

## View Switch Unit Information using EDM

Use this procedure to display switch specific information.

## Procedure steps

1. From the Device Physical View, click a switch and perform one of the following actions:
  - On the unit, right-click and select **Edit** from the drop-down list.
  - From the navigation tree, double-click **Edit** and from the Edit tree, click **Unit**.

## Field Descriptions

Use the data in this table to help you understand the switch unit display.

Name	Description
Type	Indicates the type number.
Descr	Indicates the type of switch.
Ver	Indicates the version number of the switch.
SerNum	Indicates the number of the switch.
BaseNumPorts	Indicates the base number of ports.
TotalNumPorts	Indicates the total number of ports.

---

## Unit statistics management

Use the following procedures to display and graph unit statistics using EDM.

### Display Unit Statistics

Use the following procedure to view the statistical information of a unit.

#### Procedure

1. In the **Device Physical View**, select the unit and perform one of the following actions:
  - On the unit, right-click and select **Edit** from the drop-down list.
  - From the navigation tree, double-click **Edit** and from the Edit tree, click **Unit**.
2. In the Unit work area, click the **Unit Stats** tab.

### Field Descriptions

The following table describes the fields associated with unit statistics.

Name	Description
<b>Absolute Value</b>	Indicates the counter value of packets dropped for the unit.
<b>Cumulative</b>	Indicates the total value of packets dropped seen since dialog displayed.

*Table continues...*

Name	Description
<b>Average/sec</b>	Indicates the average value of packets dropped per second.
<b>Minimum/sec</b>	Indicates the smallest value of packets dropped seen per second.
<b>Maximum/sec</b>	Indicates the largest value of packets dropped seen per second.
<b>LastVal/sec</b>	Indicates the last value of packets dropped seen per second.

## Graph Unit Statistics

Use the following procedure to graph the statistics associated with the unit.

### Procedure

- In the **Device Physical View**, select the unit and perform one of the following actions:
  - On the unit, right-click and select **Edit** from the drop-down list.
  - From the navigation tree, double-click **Edit** and from the Edit tree, click **Unit**.
- In the Unit work area, click the **Unit Stats** tab.
- On the toolbar, click **Clear Counters**.
- Select a **Poll Interval** from the drop-down list.
- In the Unit Stats section, select a data column to graph.
- On the toolbar, select **Line, Area, Bar or Pie chart**.

---

## Configuring System Parameters using the EDM

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

### Procedure steps

- From the navigation tree, double-click **Edit**.
- Double-click **Chassis**.
- In the Chassis tree, click **Chassis**.
- In the work area, click the **System** tab.
- In the **sysContact** field, type system contact information.
- In the **sysName** field, type a system name.
- In the **sysLocation** field, type a system location.
- To enable authentication traps, select the **Authentication Traps** check box.

**OR**

To disable authentication traps, clear the **Authentication Traps** checkbox.

9. In the **ReBoot** section, click a radio button.
10. In the **AutoPvid** section, click a radio button.
11. In the **StackInsertionUnitNumber** field, type a value.
12. To enable jumbo frames, select the **JumboFramesEnabled** check box.

**OR**

To disable jumbo frames, clear the **JumboFramesEnabled** checkbox.

13. To enable serial security, select the **SerialSecurityEnable** check box.
14. To enable forced stack mode, select the **ForcedStackModeEnabled** check box.
15. To enable Quick configuration, select the **QuickConfigEnable** check box.
16. In the **EdmInactivityTimeout** field, type the time-out period.
17. In the **MgmtStackIpAddress** field, type the Management stack IP address.
18. In the **StackIpv6MgmtAddress** field, type the Stack IPv6 Management address.
19. In the **StackIpv6MgmtNetMask** field, type the Stack IPv6 Management net mask address.
20. In the **Ipv6MgmtGateway** field, type the IPv6 Management Gateway address.
21. In the **BootMode** section, click a radio button.
22. Click **Apply** .

## Field Descriptions

Use the data in this table to view and modify the system level configuration.

Name	Description
sysDescr	Provides device specific information. This is a read-only item.
sysUpTime	Indicates the amount of time since the system was last booted.
sysObjectID	Indicates the system object identification number. This is a read-only item.
sysContact	Specifies contact information for the system administrator, which can include a contact name or email address.
sysName	Specifies a unique name to describe this switch.
sysLocation	Specifies the physical location of this device.
AuthenticationTraps	Enables or disables authentication traps. <ul style="list-style-type: none"> <li>• When enabled, SNMP traps are sent to trap receivers for all SNMP access authentication.</li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>When disabled, no SNMP traps are received.</li> </ul>
Reboot	<p>Provides the action to reboot the switch.</p> <ul style="list-style-type: none"> <li>running—the switch remains in the running mode</li> <li>bootPrimary—reboots the switch with the Primary image</li> <li>bootSecondary—reboots the switch with the Secondary image</li> </ul>
AutoPvid	When enabled, a VLAN ID can be automatically assigned to any port.
StackInsertionUnitNumber	<p>Specifies the unit number to assign to the next unit added to the stack. Values range from 0–8.</p> <p>You cannot set the value to the unit number of an existing stack member. When a new unit joins the stack, and the value of this object is used as its unit number, the value reverts to 0. If the value of this object is 0, it is not used to determine the unit number of new units.</p>
JumboFramesEnabled	Enables or disables the jumbo frames. When the jumbo frame is enabled, the jumbo frame size configuration for each unit or stack is applied.
JumboFrameSize	Indicates the jumbo frame size. If the <b>JumboFramesEnabled</b> check box is selected, the jumbo frame size is displayed. By default, the jumbo frame size is 9216 bytes.
SerialSecurityEnable	Enables or disables the serial security feature.
ForcedStackModeEnabled	Enables or disables the forced stack mode.
QuickConfigEnable	Enables or disables Quick Configuration.
EdmInactivityTimeout	Indicates the EDM inactivity time-out period. The value ranges from 30 to 65535 seconds. By default, the inactivity time-out period is 900 seconds.
MgmtStackIpAddress	Specifies an out-of-band management IP address for the stack.
StackIpv6MgmtAddress	Specifies an out-of-band management IP address for the stack.
StackIpv6MgmtNetMask	Specifies the subnet mask associated with the out-of-band management IP address.
Ipv6MgmtGateway	Specifies the management default gateway.
NextBootMgmtProtocol	Indicates the transport protocols to use after the next switch restart. This is a read-only item.
CurrentMgmtProtocol	Indicates the current transport protocols that the switch supports. This is a read-only item.

*Table continues...*

Name	Description
BootMode	Specifies whether to use the BootP or DHCP server to assign an IPv4 address for the management VLAN at the next switch reboot. Values include: <ul style="list-style-type: none"> <li>• other—read only</li> <li>• bootpDisabled—use configured IP address</li> <li>• bootpAlways—always use the BootP server</li> <li>• bootpWhenNeeded—use the BootP server when needed</li> <li>• bootpOrLastAddress—use BootP Server or the last time BootP assigned IP</li> <li>• dhcpAlways—use the DHCP server</li> <li>• dhcpWhenNeeded—use the DHCP server when needed</li> <li>• dhcpOrLastAddress—use DHCP Server or the last time DHCP assigned IP</li> </ul>
CurrentImageVersion	Indicates the version number of the agent image that is currently used on the switch. This is a read-only item.
NextBootDefaultGateway	Indicates the IP address of the default gateway for the agent to use after the next time you boot the switch. This is a read-only item.
CurrentDefaultGateway	Indicates the address of the default gateway that is currently in use. This is a read-only item.
NextBootLoadProtocol	Indicates the transport protocol that the agent uses to load the configuration information and the image at the next boot. This is a read-only item.
LastLoadProtocol	Indicates the transport protocol last used to load the image and configuration information about the switch. This is a read-only item.

---

## Configuring Asset ID using EDM

Use the following procedure to configure the asset ID of a switch or stack.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. On the work area, click the **Asset ID** tab.

5. In the table, double-click the cell under the **Asset ID** column heading.
6. Type the desired value in the **Asset ID** field.
7. On the toolbar, click **Apply**.

## Field Descriptions

The following table is an example for a stack of 2 units and you can extend this up to 8 units. Use the data in the following table to complete this procedure.

Name	Description
Stack	Sets the Asset ID of the stack
Unit 1	Sets the Asset ID of unit 1 in the stack
Unit 2	Sets the Asset ID of unit 2 in the stack

---

## Configuring AUR using EDM

Use this procedure to configure automatic unit replacement (AUR).

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. In the work area, select the **AUR** tab.
5. To enable automatic unit replacement, select the **AutoUnitReplacementEnabled** check box.

#### OR

To disable automatic unit replacement, clear the **AutoUnitReplacementEnabled** check box.

6. To enable automatic unit replacement save, select the **AutoUnitReplacementSaveEnabled** check box.

#### OR

To disable automatic unit replacement save, clear the **AutoUnitReplacementSaveEnabled** check box.

7. In the **AutoUnitReplacementForceSave** dialog box, type a value.
8. In the **AutoUnitReplacementRestore** dialog box, type a value.
9. Click **Apply**.

## Field Descriptions

Use the data in this table to configure AUR.

Name	Description
AutoUnitReplacementEnabled	Enables or disables the auto-unit-replacement feature.
AutoUnitReplacementSaveEnabled	Enables or disables the auto-unit-replacement automatic saving of unit images to the base unit.
AutoUnitReplacementForceSave	Forcefully saves the configuration of a particular non base unit configuration to the base unit.
AutoUnitReplacementRestore	Forcefully restores the configuration of a particular unit from the saved configuration on the base unit.

## Configuring a Switch Stack Base Unit using EDM

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

### Procedure steps

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


### Field Descriptions

Use the information in the following table to help you understand the base unit information display.

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

*Table continues...*



Name	Description
	 <b>Important:</b> In a stack configuration, the <code>reset</code> command resets only the base unit.
OperState	Indicates the operational state of the switch.
Location	Specifies the physical location of the switch.
RelPos	Indicates the relative position of the switch.
BaseNumPorts	Indicates the number of base ports of the switch.
TotalNumPorts	Indicates the number of ports of the switch.
IpAddress	Indicates the base unit IP address.
RunningSoftwareVer	Indicates the version of the running software.

## Renumbering Stack Switch Units using EDM

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

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Switch/Stack**.
4. In the work area, click the **Stack Numbering** tab.
5. To select a switch unit, click a unit row.
6. In the unit row, double-click the cell in the **New Unit Number** column.
7. Select a value from the list.
8. Click **Apply**.

A warning message appears indicating that initiating the renumbering of switch units in a stack results in an automatic reset of the entire stack.

### Field Descriptions

Use the information in the following table to change the unit numbers of switches in a stack.

Name	Description
Current Unit Number	Indicates the current switch numbering sequence.
New Unit Number	Specifies the updated switch numbering sequence.

## Managing Switch Interface Port Configurations using EDM

Use the information in this section to display and manage switch interface port configurations.

## View Switch Interface Port Information using EDM

Use this procedure to display switch interface port configuration information.

### Procedure steps


1. From the Device Physical View, select a port.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. Click **Ports**.
5. In the work area, click the **Interface** tab.

### Field Descriptions

Use the data in this table to help you understand the interface port display.

Name	Description
Index	A unique value assigned to each interface.
Name	Specifies a name for the port.
Descr	The description of the selected port.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	<p>The current administrative state of the device, 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 up state. AdminStatus changes to the down state (or remains in the up state) because either management action or the configuration information available to the managed system.</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 should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.</p>

*Table continues...*

Name	Description
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.
AutoNegotiate	Indicates whether this port is enabled for autonegotiation or not.   <b>Important:</b> 10/100BASE-TX ports can not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question.
AdminDuplex	The current administrative duplex mode of the port (half or full).
OperDuplex	The current mode of the port (half duplex or full duplex).
AdminSpeed	Set the port's speed.
OperSpeed	The current operating speed of the port.
FlowControlAdminMode	Specifies the flow control mode of the port. Values include: <ul style="list-style-type: none"> <li>• disabled — flow control disabled</li> <li>• enabledRcv — receive enabled</li> <li>• enabledXmitAndRcv — transmit and receive enabled</li> </ul>
FlowControlOperMode	Indicates the current flow control mode of the port.
AutoNegotiationCapability	Specifies the port speed and duplex capabilities that a switch can support on a port, and that can be advertised by the port using auto-negotiation.
AutoNegotiationAdvertisements	Specifies the port speed and duplex abilities to be advertised during link negotiation. Values include: <ul style="list-style-type: none"> <li>• 10Half</li> <li>• 10Full</li> <li>• 100Half</li> <li>• 100Full</li> <li>• 1000Full</li> <li>• AsymmPauseFrame</li> </ul>
MltId	The MultiLink Trunk to which the port is assigned (if any).
PortActiveComponent	Specifies the physical port components that are active for a shared port.

## Change Interface Information for Ports

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

## Procedure

1. Follow one of the following paths:
  - From the **Device Physical View**, select a port, or use Ctrl-click to select more than one port, right-click **Edit** then click the **Interface** tab.
  - From the **Device Physical View**, select a port, or use Ctrl-click to select more than one port, then follow the navigation tree to **Edit > Chassis > Ports > Interface** tab.
2. Perform one of the following:
  - If you selected a single port from Device Physical View, change parameter values by selecting the appropriate radio button for the specific parameters, then click **Apply**.
  - If you selected a group of ports from Device Physical View, you can configure parameters for specific ports by selecting the appropriate port row as in the following steps.
3. In the port row, double-click the cell in the column to be modified and configure as required from a drop-down list or by typing a value.
4. Repeat for additional cells.
5. Repeat the above steps for additional ports.
6. Click **Apply**.
7. On the toolbar, you can click **Refresh** to update the work area data display.

## Field Descriptions

Use the data in this table to modify configuration parameters for one or more interface ports.

Name	Description
Index	A unique value assigned to each interface. The value ranges between 1 and 512.
Name	Specifies a name for the port.
Descr	The description of the selected port.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	<p>The current administrative state of the device, 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 up state. AdminStatus changes to the down state (or remains in the up state) because either management action or the configuration information available to the managed system.</p>

*Table continues...*

Name	Description
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 should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.</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.
LinkTrap	Specifies whether linkUp/linkDown traps should be generated for this interface.
AutoNegotiate	<p>Indicates whether this port is enabled for autonegotiation or not.</p> <p><b>!</b> <b>Important:</b></p> <p>10/100BASE-TX ports can not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question.</p>
AdminDuplex	The current administrative duplex mode of the port (half or full).
OperDuplex	The current mode of the port (half duplex or full duplex).
AdminSpeed	Set the port speed.
OperSpeed	The current operating speed of the port.
FlowControlAdminMode	<p>Specifies the flow control mode of the port. Values include:</p> <ul style="list-style-type: none"> <li>• disabled — flow control disabled</li> <li>• enabledRcv — receive enabled</li> <li>• enabledXmitAndRcv — transmit and receive enabled</li> </ul>
FlowControlOperMode	Indicates the current flow control mode of the port.
AutoNegotiationCapability	Specifies the port speed and duplex capabilities that a switch can support on a port, and that can be advertised by the port using auto-negotiation.
AutoNegotiationAdvertisements	Specifies the port speed and duplex abilities to be advertised during link negotiation.
MltId	The MultiLink Trunk to which the port is assigned (if any).
IsPortShared	Specifies whether a port is shared. Multiple ports that are logically represented as a single port are shared. Only one shared port can be active at a time.

*Table continues...*

Name	Description
PortActiveComponent	Specifies the physical port components that are active for a shared port.

## Changing the configuration for specific interface ports using EDM


Use this procedure to modify configuration parameters for one or more interface ports.

### Procedure steps

1. From the Device Physical View, click one or more ports.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. Click **Ports**.
5. In the work area, click the **Interface** tab.
6. To select an interface port to edit, click the **Index**.
7. In the port row, double-click the cell in the **Name** column.
8. Type a character string.
9. In the port row, double-click the cell in the **AdminStatus** column.
10. Select a value from the list.
11. In the port row, double-click the cell in the **LinkTrap** column.
12. From the list, enable or disable link traps for the port.
13. In the port row, double-click the cell in the **AutoNegotiate** column.
14. Select a value from the list—**true** to enable autonegotiation for the port, or **false** to disable autonegotiation for the port.
15. In the port row, double-click the cell in the **AdminDuplex** column.
16. Select a value from the list.
17. In the port row, double-click the cell in the **AdminSpeed** column.
18. Select a value from the list.
19. In the port row, double-click the cell in the **AutoNegotiationAdvertisements** column.
20. Select or clear autonegotiation advertisement check boxes.
21. Repeat steps **6** through **20** to change the configuration for additional interface ports.
22. Click **Ok** .
23. Click **Apply** .

### Field Descriptions

Use the data in this table to modify configuration parameters for one or more interface ports.

Name	Description
Index	A unique value assigned to each interface. The value ranges between 1 and 512.
Name	Specifies a name for the port.
Descr	The description of the selected port.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	<p>The current administrative state of the device, 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 up state. AdminStatus changes to the down state (or remains in the up state) because either management action or the configuration information available to the managed system.</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 should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.</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.
LinkTrap	Specifies whether linkUp/linkDown traps should be generated for this interface.
AutoNegotiate	<p>Indicates whether this port is enabled for autonegotiation or not.</p> <p> <b>Important:</b></p> <p>10/100BASE-TX ports can not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question.</p>
AdminDuplex	The current administrative duplex mode of the port (half or full).

*Table continues...*

Name	Description
OperDuplex	The current mode of the port (half duplex or full duplex).
AdminSpeed	Set the port speed.
OperSpeed	The current operating speed of the port.
FlowControlAdminMode	Specifies the flow control mode of the port. Values include: <ul style="list-style-type: none"> <li>disabled — flow control disabled</li> <li>enabledRcv — receive enabled</li> <li>enabledXmitAndRcv — transmit and receive enabled</li> </ul>
FlowControlOperMode	Indicates the current flow control mode of the port.
AutoNegotiationCapability	Specifies the port speed and duplex capabilities that a switch can support on a port, and that can be advertised by the port using auto-negotiation.
AutoNegotiationAdvertisements	Specifies the port speed and duplex abilities to be advertised during link negotiation.
MltId	The MultiLink Trunk to which the port is assigned (if any).
IsPortShared	Specifies whether a port is shared. Multiple ports that are logically represented as a single port are shared. Only one shared port can be active at a time.
PortActiveComponent	Specifies the physical port components that are active for a shared port.

---

## Configuring Rate Limiting using EDM

Use the following procedure to configure the Rate Limiting for a single port.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Ports**.
4. On the work area, click the **Rate Limit** tab.
5. To a rate limit, click a **TrafficType** row.
6. Double-click the cell in the **AllowedRate** column.
7. Select a value from the list.
8. Double-click the cell in the **Enable** column.
9. Select a value from the list—**true** to enable the traffic type, or **false** to disable the traffic type.

### Field Descriptions

Use the data in this table to configure rate limiting.



Name	Description
TrafficType	Specifies the two types of traffic that can be set with rate limiting: broadcast and multicast.
AllowedRate	Specifies the rate limiting percentage. The available range is from 0 percent (none) to 10 percent.
AllowedRatePps	Allowed traffic rate packets/second. Values range from 0 to 262143.
Enable	Enables and disables rate limiting on the port for the specified traffic type. Options are true (enabled) or false (disabled).

## View USB Files

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

### Procedure

1. From the navigation tree, double-click **Edit**.
2. In the **Edit** tree, click **File System**.
3. In the work area, click the **USB Files** tab.

## USB Files Tab Field Descriptions

The following table defines the variables for the **Usb Files** tab.

Name	Description
Slot	Indicates the USB slot.
Name	Indicates the file name.
Date	Indicates the modification date of the file.
Size	Indicates the size of the file.

## Manage Switch Software using EDM

Use this procedure to change the binary configuration running on the switch, upload the configuration file to a TFTP server, SFTP server, or USB storage device, or retrieve a binary configuration file from a TFTP server, SFTP server, or USB storage device.

### Important:

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

### Procedure steps

1. From the navigation tree, double-click **Edit**.

2. In the Edit tree, click **File System**.
3. On the work area, click the **Config/Image/Diag file** tab.
4. In the **TftpServerInetAddressType** section, click a radio button.
5. In the **TftpServerInetAddress** dialog box, type the TFTP server IP address.
6. In the **BinaryConfigFileName** dialog box, type the name of the binary configuration file.
7. In the **BinaryConfigUnitNumber** dialog box, type a unit number.
8. In the **ImageFileName** dialog box, type the name of the current image file.
9. In the **FwFileName(Diagnostics)** dialog box, type the name of the current diagnostic file.
10. In the **UsbTargetUnit** dialog box, type a value.
11. In the **Image** section, click a radio button.
12. In the **Action** section, click a radio button.
13. Click **Apply**.

The software download starts automatically after you click Apply. This process erases the contents of flash memory, and replaces it with the new software image. Do not interrupt the download. Depending on network conditions, this process can take up to 10 minutes. After the download is complete, the switch automatically resets, and the new software image initiates a self-test. During the download, the switch is not operational.

## Field Descriptions

The following table describes the fields associated with the binary configuration running on the switch.

Name	Description
TftpServerInetAddressType	Specifies the type of IP address for the TFTP server. Values include: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
TftpServerInetAddress	Specifies the IP address of the TFTP server on which the new software images are stored for download.
BinaryConfigFileName	Specifies the binary configuration file currently associated with the switch.  Use this dialog box when you work with configuration files; do not use this dialog box when you download a software image.
BinaryConfigUnitNumber	Specifies the binary configuration unit number. Values range from 0 to 8. The default value is 0.
ImageFileName	Specifies the name of the image file currently associated with the switch. If needed, change this field to the name of the software image to be downloaded.

*Table continues...*

Name	Description
FwFileName (Diagnostics)	Specifies the name of the diagnostic file currently associated with the switch. If needed, change this field to the name of the diagnostic software image to be downloaded.
UsbTargetUnit	<p>Specifies the unit number of the USB port to be used to upload or download a file. Values range from 0 to 10.</p> <ul style="list-style-type: none"> <li>• 0—TFTP server</li> <li>• 1 to 8—a USB port in a stack</li> <li>• 9—a USB port in a standalone switch</li> <li>• 10—SFTP server</li> </ul>
Image	Specifies if the image to download is the primary or secondary image.
Action	<p>Specifies the action to take during this file system operation. The available options are as follows:</p> <ul style="list-style-type: none"> <li>• other—read only</li> <li>• dnldConfig—downloads a configuration to the switch.</li> <li>• upldConfig—uploads a configuration from the switch to a designated location.</li> <li>• dnldConfigFromUsb—downloads a configuration to switch using the front panel USB port.</li> <li>• upldConfigToUsb—uploads a configuration from the switch to the server using the front panel USB port.</li> <li>• dnldImg—downloads a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image.</li> <li>• dnldImgIfNewer—downloads a new software image to the switch only if it is newer than the one currently in use.</li> <li>• dnldImgNoReset—downloads a new software image to the switch. This option replaces the software image on the switch regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset.</li> <li>• dnldImgFromUsb—downloads a new software image to the switch using the front panel USB port.</li> <li>• dnldFw—downloads a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image.</li> <li>• dnldFwNoReset—downloads a new diagnostic software image to the switch. This option replaces the image regardless of whether it is newer or older than the current image. After the download is complete, the switch is not reset.</li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• dnldFwFromUsb—downloads a new diagnostic software image to the switch from the front panel USB port. This option replaces the image regardless of whether it is newer or older than the current image.</li> <li>• dnldImgFromUsbNoReset—downloads a new software image to the switch from the USB port and does not reset the switch.</li> <li>• dnldImgFromSftp—downloads a new software image to the switch from the SFTP server. This option replaces the software image on the switch regardless of whether it is newer or older than the current image.</li> <li>• dnldFwFromSftp—downloads a new diagnostic software image to the switch from the SFTP server. This option replaces the image regardless of whether it is newer or older than the current image.</li> <li>• dnldConfigFromSftp—downloads a configuration to the switch from the SFTP server.</li> <li>• upldConfigToSftp—uploads a configuration to the SFTP server.</li> <li>• dnldImgFromSftpNoReset—downloads the agent image from a SFTP server and does not reset the switch.</li> <li>• dnldFwFromSftpNoReset—downloads the diagnostic image from a SFTP server and does not reset the switch.</li> </ul>
Status	<p>Displays the status of the last action that occurred since the switch last booted. Values include:</p> <ul style="list-style-type: none"> <li>• other—no action occurred since the last boot.</li> <li>• inProgress—the selected operation is in progress.</li> <li>• success—the selected operation succeeded.</li> <li>• fail—the selected operation failed.</li> </ul>

## ASCII Configuration File Management using EDM

Use the information in this section to store or retrieve an ASCII configuration file.

### ASCII Configuration File Management Prerequisites

- Read and understand the detailed information about ASCII configuration files in [Using CLI and EDM on Ethernet Routing Switch 4900 and 5900 Series](#).

### Store the Current ASCII Configuration File using EDM

Use the following procedure to store the current ASCII switch configuration file to a TFTP server or USB storage device.

**! Important:**

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

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. In the work area, click the **ASCII Config Script Files** tab.
4. To select a script file, click the script index.
5. In the script row, double-click the cell in the **ScriptBootPriority** column.
6. Type a value.
7. In the script row, double-click the cell in the **ScriptSource** column.
8. Type the IP address of the desired TFTP server and the name under which to store the configuration file in the format— `tftp://<ip address>/<filename>`.

Type the IP address of the desired SFTP server and the name under which to store the configuration file in the format— `sftp://<ip address>/<filename>`.

If the configuration file is saved to a USB storage device, type the name under which to store the configuration file in the following format—`usb://<filename>`.

If the USB is inserted in a stand-alone unit, or if the USB device is inserted in a unit of a stack, type `usb://<unit number>/<filename>`.

9. Double-click the cell under the **ScriptManual** header, and select **Upload** option to transfer the file to a TFTP server or to a USB mass storage device.
10. On the toolbar, click **Apply**.
11. Check the **ScriptLastStatusChange** field for the file transfer status.
 

If the status of the file upload is `manualUploadInProgress`, wait for up to 2 minutes, and then click **Refresh** to see any new status applied to the upload.

The file upload is complete when the status displays either `manualUploadPassed` or `manualUploadFailed`.

12. Click **Apply** .

**Field Descriptions**

Use the information in the following table to help you to store the current ASCII switch configuration file.

Name	Description
ScriptIndex	Specifies the unique identifier for ASCII switch configuration file.

*Table continues...*

Name	Description
ScriptBootPriority	Specifies the boot priority of the ASCII switch configuration file. Value ranges from 0–127.
ScriptSource	Specifies the address where to store the configuration file.
ScriptManual	Specifies the operation that you want to perform—upload, download, or other.
Applications	Specifies the application.
ScriptOperStatus	Specifies the script operation status.
ScriptLastStatusChange	Specifies the time of the last status change as sysUpTime.

## Retrieve an ASCII Configuration File using EDM

Use the following procedure to retrieve an ASCII configuration file from a TFTP server or from a USB storage device, and apply it to the switch.

### Important:

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

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. On the work area, click the **ASCII Config Script Files** tab.
4. In the table, double-click the cell under the **ScriptSource** heading for the parameter you want to change.
5. Type the IP address of the desired TFTP server and the name under which to store the configuration file in the format— `tftp://<ip address>/<filename>`.

Type the IP address of the desired SFTP server and the name under which to store the configuration file in the format— `sftp://<ip address>/<filename>`.

If you retrieve the configuration file from a USB storage device, and the USB is inserted in a stand-alone unit, type the name under which to store the configuration file in the following format—`usb://<filename>`.

If the USB device is inserted in a unit of a stack, type `usb://<unit number>/<filename>`.

6. Double-click the cell under the **ScriptManual** header, and select **Download** option to transfer the file from a TFTP server or from a USB mass storage device.
7. On the toolbar, click **Apply**.
8. Check the **ScriptLastStatusChange** field for the file transfer status.

If the status of the file download is `manualDownloadInProgress`, wait for up to 2 minutes, and then click **Refresh** to see any new status applied to the upload.

The file download is complete when the status displays either **manualDownloadPassed** or **manualDownloadFailed**.

## Automatic Download of a Configuration File using EDM

Use the following procedure to download a configuration file automatically.

### Important:

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

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. On the work area, click the **ASCII Config Script Files** tab.
4. In the table, double click the cell under the **ScriptSource** header.
  - If you retrieve the configuration file from a TFTP server, type the IP address of the desired TFTP server and the name under which the configuration file is stored in the following format—`tftp://<ip address>/<filename>`.
  - If you retrieve the configuration file from a USB storage device, and the USB device is inserted in a stand-alone unit, type the name under which the configuration file is stored in the following format—`usb://<filename>`.
  - If you retrieve the configuration file from a USB storage device, and the USB device is inserted in a unit of a stack, type the name under which the configuration file is stored in the following format—`usb://<unit number>/<filename>`.
  - If you retrieve the file from a BOOTP server, type `bootp://`.
5. Double-click the cell under the **ScriptBootPriority** header.
6. Type the priority of the script (between 1 and 127, or 0 for not using the entry at boot time).
7. On the toolbar, click **Apply**.

---

## Manage the License File using EDM

Use this procedure to download, install, or remove a license file for the switch.

### Important:

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

### Load a License File from TFTP

Use this procedure to load a license file from TFTP.

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. In the work area, select the **License File** tab.

4. In the **TftpServerInetAddressType** section, click a radio button.
5. In the **TftpServerInetAddress** dialog box, type the TFTP server IP address.
6. In the LicenseFileName dialog box, enter the software license filename on the TFTP server.

**! Important:**

The LicenseFileName dialog box is case sensitive and you can use a maximum of 64 characters including the file extension. Numerals are allowed in the LicenseFileName dialog box, but special characters like @, -, #, are not allowed.

7. In the **UsbTargetUnit** dialog box, type value 0.
8. In the LicenseFileAction section, click the **dnldLicense** radio button to download license from TFTP.
9. In the **LicenseStatus** section, select the check box to remove the license.
10. Click **Apply**.

When the file installation is complete, a warning message appears prompting you to restart the switch to activate the license.

For information about restarting the switch, see [Configuring System Parameters using the EDM](#) on page 251.

## Load a License File from SFTP

Use this procedure to load a license file from SFTP.

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. In the work area, select the **License File** tab.
4. In the LicenseFileName dialog box, enter the software license filename on the SFTP server.

**! Important:**

The LicenseFileName dialog box is case sensitive and you can use a maximum of 64 characters including the file extension. Numerals are allowed in the LicenseFileName dialog box, but special characters like @, -, #, are not allowed.

5. In the **UsbTargetUnit** dialog box, type value 10.
6. In the LicenseFileAction section, click the **dnldLicenseFromSftp** radio button to download license from SFTP.
7. In the **LicenseStatus** section, select the check box to remove the license.
8. Click **Apply**.

**\* Note:**

To load a license file from an SFTP server, you must make the following configurations:

- set the SFTP server address



- set the SFTP user name
- set SFTP authentication to DSA, RSA, or password.
- if you select DSA or RSA authentication type, generate the DSA/RSA key and upload it to SFTP server
- if you select password authentication, configure the password

When the file installation is complete, a warning message appears prompting you to restart the switch to activate the license.

For information about restarting the switch, see [Configuring System Parameters using the EDM](#) on page 251.

## Load a License File from a USB Drive

Use this procedure to load a license file from a USB drive.

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **File System**.
3. In the work area, select the **License File** tab.
4. In the LicenseFileName dialog box, enter the software license filename on the USB drive.

### Important:

The LicenseFileName dialog box is case sensitive and you can use a maximum of 64 characters including the file extension. Numerals are allowed in the LicenseFileName dialog box, but special characters like @, -, #, are not allowed.

5. In the **UsbTargetUnit** dialog box, type the unit number on which the USB drive is inserted.
6. In the LicenseFileAction section, click the **dnldLicense** radio button to download license from USB.
7. In the **LicenseStatus** section, select the check box to remove the license.
8. Click **Apply**.

When the file installation is complete, a warning message appears prompting you to restart the switch to activate the license.

For information about restarting the switch, see [Configuring System Parameters using the EDM](#) on page 251.

---

## Save the Current Configuration using EDM

The configuration currently in use on a switch is regularly saved to the flash memory automatically. However, you can manually initiate this process using the **Save Configuration** tab.

Use the following procedure to save the current configuration manually.

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **File System**.
3. On the work area, click the **Save Configuration** tab.
4. Select the **AutosaveToNvramEnabled** check box to enable automatically saving the configuration to the flash memory.

### OR

Clear the **AutosaveToNvramEnabled** check box to disable automatically saving the configuration to the flash memory.

5. Choose **copyConfigToNvram** in the **Action** field.
6. On the toolbar, click **Apply**.
7. Click **Refresh**.

## Field Descriptions

Use the information in the following table to save the current configuration.

Name	Description
AutosaveToNvramEnabled	If selected, automatically saves the configuration to the flash memory.
Action	Indicates the action that you want to perform. Available options are: <ul style="list-style-type: none"> <li>• other</li> <li>• copyConfigToNvram</li> </ul>
Status	Indicates the current status.

## View Flash Information using EDM


Use the following procedure to display the currently loaded and operational agent, image, and flash load status for an individual switch or a stack.

### Procedure steps

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

### Field Descriptions

Use the data in this table to help you understand the currently loaded and operational software status display.

Name	Description
Unit	Indicates the unit number. Range is 1 to 8.
Type	Indicates the image type. Values are: <ul style="list-style-type: none"> <li>• Agent Image</li> <li>• SecondaryFlash</li> <li>• Diag Image</li> <li>• Total Flash</li> <li>• Boot Image</li> <li>• Config</li> <li>• SecondaryConfig</li> <li>• Backup Config</li> <li>• Reserved (Available)</li> <li>• MCFG</li> <li>• Audit</li> </ul>
Version	Indicates the version number.
UsedSize	Indicates the bytes used.
CurSize	Indicates the bytes allocated.
Description	Indicates the type of storage area.
Age	Indicates the number of writes to FLASH memory.
<p> <b>Important:</b></p> <p>When the currently loaded and operational software status is displayed for a stack, the unit number is replaced by the word <b>All</b>.</p>	

## Configure IPv6 Global Properties using EDM




Use the following procedure to configure IPv6 global properties.

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Globals** tab.
4. Configure the IPv6 globally.
5. On the toolbar, click **Apply** to save the changes.
6. Click **Refresh** to display updated information.

### Field Descriptions

Use the data in this table to help you configure IPv6 globally.

Name	Description
AdminEnabled	Enables or disables IPv6 administration function.
OperEnabled	Indicates the operational status of the IPv6 interface (enabled or disabled).
Forwarding	Enables or disables IPv6 routing globally. Forwarding enables IPv6 routing, notForwarding disables IPv6 routing. DEFAULT: notForwarding
DefaultHopLimit	Indicates the Hop Limit. DEFAULT: 30
IcmpNetUnreach	Enables or disables the ICMP net unreachable feature. DEFAULT: disabled
IcmpRedirectMsg	Indicates whether the ICMP redirect message feature is enabled (true) or disabled (false).
IcmpErrorInterval	Indicates the time to wait before sending an ICMP error message. A value of 0 means the system does not send an ICMP error message. Range is 0–2147483647 ms. DEFAULT: 1000
IcmpErrorQuota	Indicates the number of ICMP error messages that can be sent out during ICMP error interval. DEFAULT: 50
MulticastAdminStatus	Indicates the admin status for multicast for this interface.
Cpulpv6Address	Specifies the CPU IPv6 address for the system.   <b>Note:</b> For a standalone switch, this IP address functions as the switch IPv6 address. For a stack environment, this IP address functions as the stack IP address.   <b>Important:</b> When configured, the CPU IPv6 address takes precedence over any previously configured IPv6 addresses.
Cpulpv6NetMask	Specifies the subnet mask for the system CPU IPv6 address.
StackIpv6Address	Specifies the IPv6 address for a stack.   <b>Note:</b> A standalone switch does not permit the configuration of a stack IPv6 address.
StackIpv6NetMask	Specifies the subnet mask for the stack IPv6 address.
Ipv6DefaultGateway	Specifies the IPv6 address of the default gateway.

## IPv6 Interface Management using EDM

Use the information in this section to view, create, or delete IPv6 interfaces.

### View IPv6 Interfaces using EDM

Use the following procedure to view an IPv6 interface ID to a VLAN to learn the ID.

#### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Interfaces** tab.

#### Interfaces Tab Field Descriptions

Use the data in the following table to use the **Interfaces** tab.

Name	Description
IfIndex	Identifies a physical interface or a logical interface (VLAN). For a VLAN, it is the Ifindex of the VLAN.
Identifier	Specifies the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
IdentifierLength	Specifies the length of the interface identifier in bits.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.
VlanId	Identifies the Virtual LAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	Specifies Unicast, the only supported type.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1280.
PhysAddress	Specifies the media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false). The default is enabled (true).
OperStatus	Specifies whether the operation status of the interface is up or down.
ReachableTime	Specifies the time (3600000 ms) that a neighbor is considered reachable after receiving a reachability confirmation.
RetransmitTime	Specifies the RetransmitTime, which is the time (3600000 ms) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.
MulticastAdminStatus	Specifies the multicast status as either True or False.

### Create an IPv6 Interface using EDM

Use the following procedure to create an IPv6 interface.

## Prerequisites

- Ensure that VLAN is configured before you assign an interface identifier, or an IPv6 address to the VLAN.
- The switch supports port-based and protocol-based VLANs. For more information about configuring VLANs, see [Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 4900 and 5900 Series](#).

## Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Interfaces** tab.
4. On the toolbar, click **Insert**.
5. Configure the IPv6 interface.
6. Click **Insert**.
7. On the toolbar, click **Apply**.

## Field Descriptions

Use the data in the following table to create an IPv6 interface.

Name	Description
IfIndex	Identifies a physical interface or a logical interface (VLAN). For a VLAN, it is the Ifindex of the VLAN.
Identifier	Specifies the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. Value range is from 1280 to 9216.
AdminStatus	Specifies whether the administration status of the interface is enabled (true) or disabled (false).
ReachableTime	Specifies the time (in milliseconds) that a neighbor is considered reachable after receiving a reachability confirmation. Value range is from 1 to 3600000 ms
RetransmitTime	Specifies the RetransmitTime, which is the time (in milliseconds) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Value range is from 0 to 3600000 ms

## Delete an IPv6 Interface using EDM

Use the following procedure to delete an IPv6 interface.

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Interfaces** tab.
4. To select an interface to delete, click the **IfIndex**.
5. Click **Delete** .

---

## Graph IPv6 Interface Statistics using EDM

Use the following procedure to display and graph IPv6 interface statistics for a switch or stack.

### Procedure steps


1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Interfaces** tab.
4. In the table, select the **IfIndex** you want to view.
5. On the toolbar, click **Graph**.

## Field Descriptions

The following table defines the variables for the Static Routes window.

Name	Description
InReceives	Indicates the total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	Indicates the number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
InNoRoutes	Indicates the number of input IP datagrams discarded because no route is found to transmit them to their destination.
InAddrErrors	Indicates the number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be

*Table continues...*

Name	Description
	received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
InUnknownProtos	Indicates the number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InTruncatedPkts	Indicates the number of input IP datagrams discarded because the datagram frame did not carry enough data.
InDiscards	Indicates the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	Indicates the total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutForwDatagrams	Indicates the number of datagrams for which this entity was not their final IP destination and for which it was successful in finding a path to their final destination. In entities that do not act as IP routers, this counter will include only those datagrams that were Source-Routed through this entity, and the Source-Route processing was successful.
OutRequests	Indicates the total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	<p>Indicates the number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space).</p> <p> <b>Note:</b></p> <p>This counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.</p>
OutFragOKs	Indicates the number of IP datagrams that are successfully fragmented.

*Table continues...*



Name	Description
OutFragFails	Indicates the number of IP datagrams that are discarded because they needed to be fragmented but are not. This includes IPv4 packets that have the DF bit set and IPv6 packets that are being forwarded and exceed the outgoing link MTU.
OutFragCreates	Indicates the number of output datagram fragments that are generated because of IP fragmentation.
ReasmReqds	Indicates the number of IP fragments received which needed to be reassembled at this entity.
ReasmOKs	Indicates the number of IP datagrams successfully reassembled.
ReasmFails	Indicates the number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
InMcastPkts	Indicates the number of IP multicast datagrams received.
OutMcastPkts	Indicates the number of IP multicast datagrams transmitted.

**!** **Important:**

You can also change the **Poll Interval** by selecting and clicking on a value from the drop down list. The default value for the **Poll Interval** is 10ms.

## Graph IPv6 Interface ICMP Statistics

### About this task

Use the following procedure to display and graph the IPv6 ICMP statistics.

### Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Interfaces** tab.
4. In the table, select an interface row.
5. Click **ICMPstats**.
6. Click **Clear Counters** to reset the statistics.
7. Configure the **Poll interval** as required.

8. Highlight a data column to graph.
9. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

## ICMP Stats Tab Field Descriptions

Use the data in the following table to use the **ICMP Stats** tab.

Name	Description
AbsoluteValue	Indicates the counter value of packets dropped for the unit.
Cumulative	Indicates the total value of packets dropped seen since dialog displayed.
Average/sec	Indicates the average value of packets dropped per second.
Minimum/sec	Indicates the smallest value of packets dropped seen per second.
Maximum/sec	Indicates the largest value of packets dropped seen per second.
LastVal/sec	Indicates the last value of packets dropped seen per second.

---

## Configure an IPv6 Address using EDM

Use this procedure to configure an IPv6 address for a switch or stack.

### Procedure steps

1. From the navigation tree, double-click **IPv6** .
2. In the IPv6 tree, double-click **IPv6**.
3. In the work area, click the **Addresses** tab.
4. Click **Insert**.
5. Accept the default **IfIndex** value.  
**OR**  
 Click **Vlan** to select a vlan interface value from the list.  
**OR**  
 Click **Loopback** to select a loopback interface value from the list.
6. In the **Addr** box, type an IPv6 address.
7. In the **AddrLen** box, type the IPv6 prefix length.
8. In the **Type** section, click the **unicast** radio button if the type of address is unicast.
9. Click **Insert**.
10. Click **Apply** .

### Field Descriptions

Use the data in the following table to help you configure an IPv6 address for a switch or stack.

Name	Description
IfIndex	Specifies the index value that uniquely identifies the interface to which this entry applies.
Addr	Indicates the interface IPv6 address.
AddrLen	Indicates the interface IPv6 prefix length.
Type	Specifies the interface address type. Values include: <ul style="list-style-type: none"> <li>• unicast</li> <li>• anycast</li> </ul>
Origin	Indicates the origin of the interface address. Values include: <ul style="list-style-type: none"> <li>• other</li> <li>• manual</li> <li>• dhcp</li> <li>• linklayer</li> <li>• random</li> </ul>
Status	Indicates the status of the interface address. Values include: <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>

---

## View the IPv6 Routing Table


Use the following procedure display the IPv6 routing table.

### Procedure

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, click **IPv6**.
3. In the IPv6 work area, click the **Route** tab.

## Route Tab Field Descriptions

Use the data in the following table to use the **Route** tab.

Name	Description
<b>Dest</b>	Indicates the destination IPv6 address of the route.
<b>PfxLength</b>	Indicates the number of leading one bits that form the mask as a logical value. The prefix value must match the value in the <b>Dest</b> box. Values range from 0–128
<b>IfIndex</b>	The index value that uniquely identifies the interface to which this entry applies.
<b>NextHop</b>	Indicates the IPv6 address of the next system of a remote route.
<b>Type</b>	<p>Indicates the IPv6 route type.</p> <ul style="list-style-type: none"> <li>• discard: Indicates that packets to destinations matching this route are to be discarded.</li> <li>• local: Indicates a route for which the next hop is the final destination.</li> <li>• remote: Indicates a route for which the next hop is not the final destination.</li> </ul>
<b>Protocol</b>	<p>Indicates the IPv6 route protocol.</p> <p>Values include:</p> <ul style="list-style-type: none"> <li>• other: none of the following</li> <li>• local: Indicates non-protocol information such as manually configured entries.</li> <li>• netmgmt: Indicates the static route</li> <li>• ndisc: Indicates the value obtained from the Neighbor Discovery protocol.</li> </ul>
<b>Policy</b>	<p>Indicates the IPv6 route policy which sets conditions that would cause the selection of a multipath route.</p> <p> <b>Note:</b> Unless the mechanism indicated by the IPv6 route protocol specifies otherwise, the policy specifier is the 8-bit Traffic Class field of the</p>

*Table continues...*

Name	Description
	IPv6 packet header that is zero extended at the left to a 32-bit value.
<b>Age</b>	Indicates the time, in seconds, since the IPv6 route was last updated.
<b>NextHopRDI</b>	Indicates the Routing Domain ID of the next hop of this route.  * <b>Note:</b> When this object is unknown or not relevant, this value is set to zero.
<b>Metric</b>	Indicates the IPv6 route metric. Determined by the routing protocol specified in the IPv6 route protocol value.  * <b>Note:</b> When this object is unknown or not relevant to the protocol indicated by the IPv6 route protocol, the object value is the maximum value (4,294,967,295).
<b>Weight</b>	Indicates the system internal weight for this route.

## Configure an IPv6 Discovery Prefix

Use the following procedure to configure an IPv6 discovery prefix.

### About this task

The IPv6 discovery prefix determines the source of an IP address or set of IP addresses. The discovery prefix also permits other tables to share the information through a pointer rather than by copying. For example, when the node configures both a unicast and anycast address for a prefix, the `ipAddressPrefix` objects for those addresses point to a single row in the table.

### Procedure

1. From the navigation tree, double-click **IPv6**.
2. Double-click **IPv6**.
3. Click the **Discovery Prefix** tab.
4. Click **Insert**.
5. In the **IfIndex** box, click **VLAN**, and select a VLAN.
6. Edit the remaining fields.
7. Click **Insert**.
8. On the toolbar, click **Apply**.

9. On the toolbar, you can click **Refresh** to verify the configuration.

**\* Note:**

You can also configure an IPv6 discovery prefix for a particular VLAN from the navigation path **VLAN > VLANs** , select a VLAN row, and select **IPv6 > IPv6 Discovery Prefix**.

## Discovery Prefix Tab Field Descriptions

Use the data in the following table to use the **Discovery Prefix** tab.

Name	Description
<b>IfIndex</b>	A read-only value indicating the unique value to identify an IPv6 interface.
<b>Prefix</b>	Configures the prefix to create an IPv6 address in the IPv6 interface table.
<b>PrefixLen</b>	Configures the mask to create an IPv6 prefix entry as either advertised or suppressed.
<b>VlanId</b>	Specifies the VLAN ID of the IPv6 interface.
<b>UseDefaultVal</b>	Select one of the values to set its value to default value. This is a bitmask field, setting all the bits means that all the options will be reverted to default values.
<b>ValidLife</b>	Configures the valid lifetime in seconds that indicates the length of time this prefix is advertised. The default is 2592000.
<b>PreferredLife</b>	Configures the preferred lifetime in seconds that indicates the length of time this prefix is advertised. The default value is 604800.
<b>Infinite</b>	Configures the prefix valid lifetime so it never expires. The default is false.
<b>OnLinkFlag</b>	Configures the prefix for use when determining if a node is onlink. This value is placed in the L-bit field in the prefix information option. It is a 1-bit flag. The default is true.
<b>AutoFlag</b>	Configures the prefix for use as the autonomous address configuration. This value is placed in the autoflag field in the prefix information option. It is a 1-bit flag. The default is true.
<b>AddressEui</b>	Configures the EUI address. Use an EUI-64 interface ID in the low-order 64-bits of the address when the ID is not specified in the address field. If enabled, use EUI, or use EUI-64 and the complement Universal/Local (U/L) bit. This operation provides for both global and link-local addresses. After you create

*Table continues...*

Name	Description
	the entry, you cannot modify this value. This value is valid for use only when the PrefixLength is 64 or less. The default is eui-not-used.
<b>NoAdvertise</b>	Select true to not include the prefix in the neighbor advertisement. The default is false.

## Configure IPv6 Router Advertisement

IPv6 nodes on the same link use Neighbor Discovery Protocol (NDP) to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. NDP combines the services provided by Address Resolution Protocol (ARP) and router discovery for IPv4.

Use the following procedure to configure router advertisement in IPv6 for Neighbor Discovery Protocol (NDP).

### Procedure

1. From the navigation pane, double-click **IPv6**.
2. Double-click **IPv6**.
3. In the **IPv6** work area, click the **Route Advertisement** tab.
4. Edit the fields as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the configuration.

#### **Note:**

You can also configure an IPv6 router advertisement for a particular VLAN from the navigation path **VLAN > VLANs** , select a VLAN row, and select **IPv6 > Route Advertisement**.

## Router Advertisement Tab Field Descriptions

Use the data in the following table to use the **Router Advertisement** tab.

Name	Description
<b>IfIndex</b>	A unique value to identify a physical interface or a logical interface (VLAN).
<b>SendAdverts</b>	Indicates whether the router sends periodic router advertisements and responds to router solicitations on this interface. The default is True.

*Table continues...*

Name	Description
<b>UseDefaultVal</b>	Select one included value to use the default value, or use all bits to configure all options to their default value.
<b>MaxInterval</b>	Configure the maximum interval (in seconds) at which the transmission of router advertisements occurs on this interface. This must be no less than 4 seconds and no greater than 1800 seconds. The default is 600.
<b>MinInterval</b>	Configure the minimum interval (in seconds) at which the transmission of router advertisements can occur on this interface. The value must be no less than 3 seconds and no greater than $.75 \times \text{max-interval}$ . The default is 200.
<b>ReachableTime</b>	The value (in milliseconds) placed in the router advertisement message sent by the router. Configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event. The default is 30000.
<b>RetransmitTimer</b>	The value (in milliseconds) placed in the retransmit timer field in the router advertisement message sent from this interface. The value zero means unspecified (by this router). The value configures the amount of time that router waits for the transmission to occur. The default is 1000.
<b>DefaultLifeTime</b>	The value placed in the router lifetime field of router advertisements sent from this interface. This value must be either 0 or between <code>rcIpv6RouterAdvertMaxInterval</code> and 9000 seconds. A value of zero indicates that the router is not a default router. The default is 3 times the value of <code>rcIpv6RouterAdvertMaxInterval</code> or 1800.
<b>CurHopLimit</b>	The default value placed in the current hop limit field in router advertisements sent from this interface. The value must be the current diameter of the Internet. A value of zero in the router advertisement indicates that the advertisement is not specifying a value for <code>urHopLimit</code> . The value must be the value specified in the IANA Web pages ( <a href="http://www.iana.org">www.iana.org</a> ). The default is 30.
<b>ManagedFlag</b>	If enabled, the <code>ManagedFlag</code> configures the M-bit or the managed address configuration in the router advertisement. The default is false.
<b>OtherConfigFlag</b>	If set to true, then the O-bit (Other stateful configuration) in the router advertisement is set.

*Table continues...*



Name	Description
	Reference RFC2461 Section 6.2.1. The default value is false.
<b>DadNSNum</b>	The number of neighbor solicitation messages for duplicate address detection (DAD). A value of 0 disables the DAD process on this interface. A value of 1 sends one advertisement without retransmissions.
<b>LinkMTU</b>	The value placed in MTU options sent by the router on this interface. A value of zero indicates that the router sends no MTU options.

## IPv6 Neighbor Cache Management using EDM

Use the information in this section to view and configure the IPv6 neighbor cache.

### View the IPv6 Neighbor Cache using EDM

View the neighbor cache to discover information about neighbors in the network. Neighbor cache in IPv6 is similar to the IPv4 Address Resolution Protocol (ARP) table. The neighbor cache is a set of entries for individual neighbors to which traffic was sent recently. You make entries on the neighbor on-link unicast IP address, including information such as the link-layer address. A neighbor cache entry contains information used by the Neighbor Unreachability Detection algorithm, including the reachability state, the number of unanswered probes, and the time the next Neighbor Unreachability Detection event is scheduled.

#### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Neighbors** tab.

#### Neighbors Tab Field Descriptions

Use the data in the following table to use the **Neighbors** tab.

Name	Description
IfIndex	Specifies a unique Identifier of a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN.
NetAddress	Indicates the IP address corresponding to the media-dependent physical address.
PhysAddress	Indicates the media-dependent physical address. The range is 0–65535. For Ethernet, this is a MAC address.

*Table continues...*

Name	Description
Interface	Indicates either a physical port ID or the Multi-Link Trunking port ID. This entry is associated either with a port or with the Multi-Link Trunking in a VLAN.
LastUpdated	Specifies the value of sysUpTime at the time this entry was last updated. If this entry was updated prior to the last reinitialization of the local network management subsystem, this object contains a zero value.
Type	<p>Specifies the types of mapping.</p> <ul style="list-style-type: none"> <li>• Dynamic type—indicates that the IP address to the physical address mapping is dynamically resolved using, for example, IPv4 ARP or the IPv6 Neighbor Discovery Protocol.</li> <li>• Static type—indicates that the mapping is statically configured.</li> <li>• Local type—indicates that the mapping is provided for the interface address.</li> </ul> <p>The default is static.</p>
State	<p>Specifies the Neighbor Unreachability Detection state for the interface when the address mapping in this entry is used. If Neighbor Unreachability Detection is not in use (for example, for IPv4), this object is always unknown. Options include the following:</p> <ul style="list-style-type: none"> <li>• reachable—confirmed reachability</li> <li>• stale—unconfirmed reachability</li> <li>• delay—waiting for reachability confirmation before entering the probe state</li> <li>• probe—actively probing</li> <li>• invalid—an invalidated mapping</li> <li>• unknown—state cannot be determined</li> <li>• incomplete—address resolution is being performed</li> </ul>

## Configure the IPv6 Neighbor Cache using EDM

Use the following procedure to configure the IPv6 neighbor cache.

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**
3. On the work area, click the **Neighbors** tab.

4. On the toolbar, click **Insert**.
5. Configure the parameters as required.
6. Click **Insert**.
7. Click **Apply**.

## Field Descriptions

Use the data in the following table to list the fields in the **Insert Neighbors** dialog box.

Name	Description
IfIndex	Indicates a unique identifier to a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN.
NetAddress	Indicates the IP address corresponding to the media-dependent physical address.
PhysAddress	Indicates the media-dependent physical address. The range is 0–65535. For Ethernet, this is a MAC address.
Interface	Indicates either a physical port ID or the Multi-Link Trunking port ID. This entry is associated either with a port or with the Multi-Link Trunking in a VLAN.

## Delete the IPv6 Neighbor Cache using EDM

Use this procedure to delete the IPv6 neighbor cache.

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **Neighbors** tab.
4. To select an cache to delete, click the **IfIndex**.
5. Click **Delete** .

---

## Graph IPv6 Interface ICMP Statistics using EDM

Use the following procedure to display and graph the IPv6 ICMP statistics.

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **IPv6**.
3. On the work area, click the **ICMP Stats** tab.
4. Click **Clear Counters** to reset the statistics.
5. Configure the **Poll interval** as required.
6. Highlight a data column to graph.

- On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

## ICMP Stats Tab Field Descriptions

Use the data in the following table to use the **ICMP Stats** tab.

Name	Description
AbsoluteValue	Indicates the counter value of packets dropped for the unit.
Cumulative	Indicates the total value of packets dropped seen since dialog displayed.
Average/sec	Indicates the average value of packets dropped per second.
Minimum/sec	Indicates the smallest value of packets dropped seen per second.
Maximum/sec	Indicates the largest value of packets dropped seen per second.
LastVal/sec	Indicates the last value of packets dropped seen per second.

## View ICMP Message Statistics using EDM

Use the following procedure to display the IPv6 interface ICMP message statistics.

### Procedure steps

- From the navigation tree, double-click **IPv6**.
- In the IPv6 tree, double-click **IPv6**.
- On the work area, click the **ICMP Msg Stats** tab.
- On the toolbar, click **Refresh** to update the ICMP message statistics.

### Field Descriptions

Use the data in the following table to display ICMP message statistics.

Name	Description
Type	Indicates the type of packet received or sent.
InPkts	Indicates the number of packets received.
OutPkts	Indicates the number of packets sent.

## Display IPv6 TCP Global Properties using EDM

Use the following procedure to display IPv6 TCP global properties.

### Procedure steps

- From the navigation tree, double-click **IPv6**.
- In the IPv6 tree, double-click **TCP/UDP**.

3. On the work area, click the **TCP Globals** tab.
4. Click **Refresh** to update the information.

## Field Descriptions

Use the data in the following table to display IPv6 TCP global properties.

Name	Description
RtoAlgorithm	Indicates the algorithm identifier.
RtoMin	Indicates the minimum value in milliseconds.
RtoMax	Indicates the maximum value in milliseconds.
MaxConn	Indicates the maximum number of connections.

---

## Display IPv6 TCP Connections using EDM

Use the following procedure to display IPv6 TCP connections.

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **TCP/UDP**.
3. On the work area, click the **TCP Connections** tab.
4. Click **Refresh** to update the information.

## Field Descriptions

Use the data in the following table to display IPv6 TCP connections.

Name	Description
LocalAddressType	Indicates the type of the local address.
LocalAddress	Indicates the local address.
LocalPort	Indicates the local port.
RemAddressType	Indicates the type of the remote address.
RemAddress	Indicates the remote address.
RemPort	Indicates the remote port.
State	Enables or disables the state.

---

## Display IPv6 TCP Listeners using EDM

Use the following procedure to display IPv6 TCP listeners.

## Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **TCP/UDP**.
3. On the work area, click the **TCP Listeners** tab.
4. Click **Refresh** to update the information.

## Field Descriptions

Use the data in the following table to display IPv6 TCP listeners.

Name	Description
LocalAddressType	Indicates the local IP address type. Values include IPv4 or IPv6.
LocalAddress	Indicates the local IPv4 or IPv6 address.
Local Port	Indicates the local port.

---

## Display IPv6 UDP Endpoints using EDM

Use the following procedure to display IPv6 UDP endpoints.

### Procedure steps

1. From the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, double-click **TCP/UDP**.
3. On the work area, click the **UDP Endpoints** tab.
4. Click **Refresh** to update the information.

## Field Descriptions

Use the data in the following table to display IPv6 UDP endpoints.

Name	Description
LocalAddressType	Indicates the local address.
LocalAddress	Indicates the local address port.
Local Port	Indicates the local port.
RemoteAddressType	Indicates the remote address type.
RemoteAddress	Indicates the remote address.
RemotePort	Indicates the remote port.
Instance	Indicates the instance.
Process	Indicates the process.

---

## View SFP GBIC Ports using EDM

Use the following procedure to view the SFP GBIC ports.

### Procedure steps

1. From the **Device Physical View**, click a unit.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double click **Chassis**.
4. In the Chassis tree, double-click **Ports**.

---

## View Basic System Bridge Information using EDM

Use this procedure to display system bridge information, including the MAC address, type, and number of ports participating in the bridge.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **Base** tab.

### Field Descriptions

Name	Description
BridgeAddress	Indicates the MAC address of the bridge when it is uniquely referred to. This address must be the smallest MAC address of all ports that belong to the bridge. However, it must be unique. When concatenated with dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol.
NumPorts	Indicates the number of ports controlled by the bridging entity.
Type	Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this fact is indicated by entries in the port table for the given type.

---

## Initiate a Cable Diagnostic Test using EDM

Use this procedure to initiate and display results for a cable diagnostic test on a specific switch port, using the Time Domain Reflectometer (TDR).

### Procedure steps

1. From the **Device Physical View** right-click a port.

2. Click **Edit**.
3. In the work area, click the **TDR** tab.
4. Select the **StartTest** check box.
5. Click **Apply**.

## Field Descriptions

Use the data in the following table to initiate a cable diagnostic test and help you understand the TDR display.

Name	Description
StartTest	When selected, enables the cable diagnostic test.
TestDone	Indicates whether the TDR test is complete (true) or not (false).
CableStatus	Indicates the status of the cable as a summation of the status of the cable conductor pairs. <ul style="list-style-type: none"> <li>• 1—Fail: the cable is experiencing any combination of open and shorted pairs</li> <li>• 2—Normal: the cable is operating normally with no fault found</li> </ul>
CableLength	Indicates the length of cable, in meters, based on average electrical length of 4 pairs. This measurement can be performed whether or not network traffic is present on the cable.
Pair1Status	Indicates the status of the first pair in the cable. Values include: <ul style="list-style-type: none"> <li>• 1—pairFail</li> <li>• 2—pairNormal</li> <li>• 3—pairOpen</li> <li>• 4—pairShorted</li> <li>• 5—pairNotApplicable</li> <li>• 6—pairNotTested</li> <li>• 7—pairForce</li> <li>• 8—pinShort</li> </ul> <p><b>!</b> <b>Important:</b></p> <p>If a 10MB or 100MB link is established without autonegotiation, Pair 1 returns Forced mode. The pair length is meaningless in this case.</p>
Pair1Length	Indicates the length of the first pair in the cable, in meters, measured by the TDR.

*Table continues...*



Name	Description
Pair2Status	Indicates the status of the second pair in the cable. Values include: <ul style="list-style-type: none"> <li>• 1—pairFail</li> <li>• 2—pairNormal</li> <li>• 3—pairOpen</li> <li>• 4—pairShorted</li> <li>• 5—pairNotApplicable</li> <li>• 6—pairNotTested</li> <li>• 7—pairForce</li> <li>• 8—pinShort</li> </ul>
Pair2Length	Indicates the length of the second pair in the cable, in meters, measured by the TDR.
Pair3Status	Indicates the status of the third pair in the cable. Values include: <ul style="list-style-type: none"> <li>• 1—pairFail</li> <li>• 2—pairNormal</li> <li>• 3—pairOpen</li> <li>• 4—pairShorted</li> <li>• 5—pairNotApplicable</li> <li>• 6—pairNotTested</li> <li>• 7—pairForce</li> <li>• 8—pinShort</li> </ul>
Pair3Length	Indicates the length of the third pair in the cable, in meters, measured by the TDR.
Pair4Status	Indicates the status of the fourth pair in the cable. Values include: <ul style="list-style-type: none"> <li>• 1—pairFail</li> <li>• 2—pairNormal</li> <li>• 3—pairOpen</li> <li>• 4—pairShorted</li> <li>• 5—pairNotApplicable</li> <li>• 6—pairNotTested</li> <li>• 7—pairForce</li> <li>• 8—pinShort</li> </ul>

*Table continues...*

Name	Description
Pair4Length	Indicates the length of the third pair in the cable, in meters, measured by the TDR.

## View Transparent Bridge Information using EDM

Use the following procedure to display information about learned forwarding entry discards and to configure the aging time and MAC learning.

### Procedure Steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **Transparent** tab.
4. In the **AgingTime** dialog box, type a value.
5. To select a port to enable learning, click the **MacAddrTableLearningPorts** ellipsis.
6. To enable MAC learning, select one or more port numbers.

OR

To disable MAC learning, deselect one or more port numbers.

#### \* **Note:**

If you disable or enable a port that is part of an active MLT trunk or has the same LACP key, you also disable or enable the other ports in the trunk so that all ports in the trunk share the same behavior.


7. Click **Ok**.
8. On the tool bar, click **Apply**.

### Field Descriptions

The following table describes the fields associated with information about MAC learning.

Name	Description
LearnedEntryDiscards	Indicates the number of Forwarding Database entries learned that are discarded due to insufficient space in the Forwarding Database. If this counter increases, it indicates that the Forwarding Database is becoming full regularly. This condition affects the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has occurred but is not persistent.
AgingTime	Indicates the time-out period in seconds for removing old dynamically learned forwarding information.

*Table continues...*

Name	Description
	 <b>Important:</b> The 802.1D-1990 specification recommends a default of 300 seconds.
MacAddrTableLearningPorts	Specifies the ports which are enabled for MAC learning.

## View Forwarding Bridge Information using EDM

Use this procedure to display information about bridge forwarding status.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Bridge**.
3. On the work area, click the **Forwarding** tab.
4. To select specific bridge port status information display criteria, click **Filter**.
5. Select filtering criteria.
6. Click **Filter**.

### Field Descriptions

Use the data in the following table to help you understand the bridge port status display.

Name	Description
Id	Specifies the VLAN identifier.
Address	Indicates the unicast MAC address for which the bridge has forwarding or filtering information.
Port	<p>Indicates the port number. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress</p> <p>A value of 0 indicates that the port number has not been learned, so the bridge does not have the forwarding or filtering information for this address (in the dot1dStaticTable). You must assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned.</p>
Status	<p>Indicates the values for this field include:</p> <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> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• other: None of the preceding. This includes instances where another MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is used to determine if frames addressed to the value of dot1dTpFdbAddress are being forwarded.</li> </ul>

## Graph Port Bridge Statistics using EDM

Use the following procedure to graph port bridge statistical information.

### Procedure steps

1. From the Device Physical View, click a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Bridge** tab.
5. On the toolbar, select a value from the **Poll Interval** list.
6. To reset the statistics counters, click **Clear Counters**.
7. To select bridge statistical information to graph, click a data row under a column heading.
8. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart** column.

### Field Descriptions

Use the data in the following table to help you understand port bridge statistics.

Name	Description
DelayExceededDiscards	Number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges.
MtuExceededDiscards	Number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges.
InFrames	The number of frames that have been received by this port from its segment.
OutFrames	The number of frames that have been received by this port from its segment.
InDiscards	Count of valid frames received which were discarded (filtered) by the Forwarding Process.

## Configure SNTP using EDM

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

## Procedure steps

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

## Field Descriptions

Use the data in this table to configure SNTP.

Name	Description
PrimaryServerInetAddress Type	Specifies the primary SNTP server IP address type. Values include ipv4 and ipv6.
PrimaryServerInetAddress	Specifies the IP address of the primary SNTP server.
SecondaryServerInetAddress Type	Specifies the secondary SNTP server IP address type. Values include ipv4 and ipv6.
SecondaryServerInetAddress	Specifies the IP address of the secondary SNTP server.
State	Specifies if the switch uses SNTP to synchronize the switch clock to the Coordinated Universal Time (UTC). <ul style="list-style-type: none"> <li>• disabled—the device cannot synchronize its clock using SNTP</li> <li>• enabled (unicast)—the device synchronizes to UTC shortly after start time when network access becomes available, and periodically thereafter</li> </ul>
SyncInterval	Specifies the frequency, in hours, that the device attempts to synchronize with the NTP servers. Values range from 0 to 168. With a value of 0, synchronization occurs only when the switch boots up.
ManualSyncRequest	Specifies that the device to immediately attempt to synchronize with the NTP servers.

*Table continues...*

Name	Description
LastSyncTime	Indicates the Coordinated Universal Time (UTC) when the device last synchronized with an NTP server. This is a read-only value.
LastSyncSourceInetAddress Type	Indicates the IP source address type of the NTP server with which this device last synchronized.
LastSyncSourceInetAddress	Indicates the IP source address of the NTP server with which this device last synchronized. This is a read-only value.
NextSyncTime	Indicates the UTC at which the next synchronization is scheduled.
PrimaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the primary server address. However, synchronization with the secondary server address can still occur.
SecondaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the secondary server address,
CurrentTime	Indicates the current switch UTC.

## Configure the Local Time Zone using EDM

Use the following procedure to set a local time zone.

### Procedure steps

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

### Field Descriptions

The following table describes the Time Zone screen fields.

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

## Configure Daylight Savings Time using EDM

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

## Prerequisites

- Disable the summer time recurring feature.

## Procedure steps

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

### OR

Clear the **Enabled** check box to disable daylight saving time for the switch.


17. Click **Apply** .

## Field Descriptions

Use the data in this table to configure the start and end of the daylight saving time period.

Name	Description
Offset	Specifies the time in minutes by which you want to change the time when daylight savings begins and ends. The offset is added to the current time when daylight saving time begins and subtracted from the current time when daylight saving time ends.
TimeZoneAcronym	Specifies a time zone acronym.
StartYear	Specifies the year from when you want to start the daylight savings time.

*Table continues...*

Name	Description
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.
EndMinutes	Specifies the minute of the particular hour when to end the daylight savings time.
Enabled	<p>Enables or disables daylight saving time.</p> <p> <b>Important:</b> Before you enable daylight saving time, configure the feature attributes.</p>

## Configure Recurring Daylight Saving Time using EDM

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

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **SNTP/Clock**.
3. In the work area, click the **Summer Time Recurring** tab.
4. Select the **Recurring** check box to enable recurring daylight saving time for the switch.

#### OR

- Clear the **Recurring** check box to disable recurring daylight saving time for the switch.
5. In **RecurringStartMonth**, make a selection from the drop-down list.
  6. In **RecurringStartWeek**, click a button.
  7. In **RecurringStartDay**, make a selection from the drop-down list.



8. In **RecurringStartHour**, make a selection from the drop-down list.
9. In the **RecurringStartMinute** dialog box, type a value from 0 to 59.
10. In **RecurringEndMonth**, make a selection from the drop-down list.
11. In **RecurringEndWeek**, click a button.
12. In **RecurringEndDay**, make a selection from the drop-down list.
13. In **RecurringEndHour**, make a selection from the drop-down list.
14. In the **RecurringEndMinute** dialog box, type a value from 0 to 59.
15. In the **RecurringOffset** dialog box, type a value from 1 to 1440.
16. On the tool bar, click **Apply**.

## Field Descriptions

Use the data in this table to configure recurring daylight saving time.

Name	Description
Recurring	When selected, enables daylight saving time to recur yearly.
RecurringStartMonth	Specifies the month of each year you want recurring daylight savings time to start.
RecurringStartWeek	Specifies the week of the month you want recurring daylight savings time to start. Week 5 may not apply in certain years. In that case summer time start falls back to the 'last' option. For example: in a year where there is no Sunday in the fifth week of March, summer time will start on the last Sunday of March.
RecurringStartDay	Specifies the day of the particular month you want recurring daylight savings time to start.
RecurringStartHour	Specifies the hour of the particular day you want recurring daylight savings time to start.
RecurringStartMinute	Specifies the minutes of the particular hour you want recurring daylight savings time to start.
RecurringEndMonth	Specifies the month of each year you want recurring daylight savings time to end.
RecurringEndWeek	Specifies the week of the month you want recurring daylight savings time to end. Week 5 may not apply in certain years. In that case summer time start falls back to the 'last' option. For example: in a year where there is no Sunday in the fifth week of October, summer time will end on the last Sunday of October.
RecurringEndDay	Specifies the day of the particular month you want recurring daylight savings time to end.

*Table continues...*

Name	Description
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.

---

## Link-State Configuration using EDM

Use the following procedure to configure link-state using EDM.

### Enable Link-State Tracking

#### About this task

Link-state tracking (LST) binds the link state of multiple interfaces. The association between the upstream and downstream interfaces form link-state tracking group.

To enable link-state tracking, create a link-state group, and specify the interfaces that are assigned to the link-state group. The downstream interfaces are bound to the upstream interfaces. After assigning the upstream and downstream interfaces, enable the link-state group.

#### Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, double-click **Edit**.
3. In the Edit tree, click **Link State Tracking**.
4. On the **Link State Tracking** tab, click the **GroupId** to select the group.
5. In the **GroupId** row, double-click the cell in the **UpstreamPortList** column.
6. Select the ports and click **Ok**.
7. Double-click the cell in the **DownstreamPortList** column.
8. Select the ports and click **Ok**.
9. Double-click the cell in the **UpstreamMLTList** column.
10. Select the trunks and click **Ok**.
11. Double-click the cell in the **DownstreamMLTList** column.
12. Select the trunks and click **Ok**.
13. Double-click the cell in the **Enabled** column.

14. Click **true** to enable the selected group.
15. The **OperState** displays if the tracking group configuration status.
16. Click **Apply**, to save the configuration.

## Field Descriptions

The following table describes the variables for the Link State Tracking window.

Name	Description
<b>GroupId</b>	Specifies the link-state tracking group ID.
<b>Enabled</b>	Specifies if the link-state group is enabled or not. Values are: <ul style="list-style-type: none"> <li>• true</li> <li>• False</li> </ul>
<b>UpstreamPortList</b>	Specifies the ports that can be added to the link-state group as up stream ports.
<b>DownstreamPortList</b>	Specifies the ports that can be added to link-state group as down stream ports.
<b>UpstreamMltList</b>	Specifies the trunks that can be added to the up stream MLT list.
<b>DownstreamMltList</b>	Specifies the trunks that can be added to the down stream MLT list.
<b>OperState</b>	Displays the operating status of the link-state group.

---

## View Network Topology Information using EDM

Use this procedure to display network topology information.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **Topology**.
4. In the work area, click the **Topology** tab.
5. In the **Status** section, click a radio button..
6. Click **Apply** .

### Field Descriptions

Use the data in this table to help you understand the topology display.

Name	Description
IpAddr	Indicates the IP address of the device.
Status	Specifies whether topology is on (topOn) or off (topOff) for the device. The default value is topOn.
NmmLstChg	Indicates the value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent.
NmmMaxNum	Indicates the maximum number of entries in the NMM topology table.
NmmCurNum	Indicates the current number of entries in the NMM topology table.

## View the Topology Table using EDM

Use this procedure to display the topology table.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **Topology**.
4. In the work area, click the **Topology Table** tab.

### Field Descriptions

Use the data in this table to help you understand the topology table display.

Name	Description
Slot	Indicates the slot number in the chassis in which the topology message was received.
Port	Indicates the port on which the topology message was received.
IpAddr	Indicates the IP address of the sender of the topology message.
SegId	Indicates the segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	Indicates the MAC address of the sender of the topology message.
ChassisType	Indicates the chassis type of the device that sent the topology message.
BkplType	Indicates the backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	Indicates the current state of the sender of the topology message. The choices are: <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>

## Enable or Disable TLV Transmit Flags using EDM

Use this procedure to enable or disable the transmission of optional proprietary TLVs from switch ports to IP phones.


### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Port Config** tab.
6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **TLVsTxEnable** column.
8. Select a checkbox to enable a TLV.

### OR

- Clear a checkbox to disable a TLV.
9. Click **Ok**.
  10. On the toolbar, click **Apply**.

### Field Descriptions

Name	Description
poeConservationLevel	Enables or disables the TLV for requesting a specific power conservation level for an IP phone connected to the switch port.   <b>Important:</b> Only Ethernet ports on switches that support PoE can request a specific power conservation level for an IP phone.
callServer	Enables or disables the TLV for advertising call server IPv4 addresses to an IP phone connected to the switch port.
fileServer	Enables or disables the TLV for advertising file server IPv4 addresses to an IP phone connected to the switch port.
framingTlv	Enables or disables the frame tagging TLV for exchanging Layer 2 priority tagging information between the switch and an IP phone.
faElementType	Enables or disables the TLV for advertising Fabric Attach operation to Fabric Attach-capable devices connected to the switch port.

*Table continues...*

Name	Description
falsidVlanAsgns	Enables or disables the TLV for advertising Fabric Attach I-SID/VLAN assignments to a Fabric Attach-capable device connected to the switch port.
faZeroTouch	Enables or disables the TLV for advertising Fabric Attach Zero Touch settings to a Fabric Attach-capable device connected to the switch port.


## View the TLV Transmit Flag Status using EDM

Use this procedure to display the status of transmit flags for switch ports on which IP phone support TLVs are configured.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Port Config** tab.

### Field Description

Name	Description
poeConservationLevel	When displayed, indicates that the TLV for requesting a specific power conservation level for an IP phone is enabled on the switch port.   <b>Important:</b> Only Ethernet ports on switches that support PoE can request a specific power conservation level for an IP phone.
callServer	When displayed, indicates that call server IPv4 address advertisement to an IP phone is enabled on the switch port.
fileServer	When displayed, indicates that file server IPv4 address advertisement to an IP phone is enabled on the switch port.
framingTlv	When displayed, indicates that frame tagging is enabled on the port, for exchanging Layer 2 priority tagging information between the switch and an IP phone.
faElementType	When displayed, indicates that Fabric Attach advertisement to a Fabric Attach-capable device is enabled on the switch port.
falsidVlanAsgns	When displayed, indicates that Fabric Attach I-SID/VLAN assignments advertisement to a Fabric Attach-capable device is enabled on the switch port.
faZeroTouch	When displayed, indicates that Fabric Attach Zero Touch advertisement to a Fabric Attach-capable device is enabled on the switch port.

## Configure the Switch Call Server IP Address TLV using EDM

Use this procedure to define the local call server IP addresses that switch ports can advertise to IP phones.

You can define IP addresses for a maximum of 8 local call servers.

### Important:

The switch does not support the advertisement of IPv6 addresses to IP phones.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Local Call Servers** tab.
6. To select a port, click the **CallServerNum**.
7. In the port row, double-click the cell in the **CallServerAddress** column.
8. Type an IP address in the box.
9. On the toolbar, click **Apply**.

### Field Descriptions

Name	Description
CallServerNum	Displays the call server number.
CallServerAddressType	Displays the call server IP address type.
CallServerAddress	Defines the local call server IP address to advertise.

## View the Switch Call Server IP address TLV Configuration using EDM

Use this procedure to display information about the defined local call server IP addresses that switch ports can advertise to IP phones.

### Important:

The switch does not support the advertisement of IPv6 addresses to IP phones.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.

- In the work area, click the **Local Call Servers** tab.

### Field Descriptions

Name	Description
CallServerNum	Displays the call server number.
CallServerAddressType	Displays the call server IP address type.
CallServerAddress	Displays the defined call server IP address.

## Configure the Switch File Server IP Address TLV using EDM

Use this procedure to define the local file server IP addresses that switch ports can advertise to IP phones.

You can define IP addresses for a maximum of 4 local call servers.

### \* Note:

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

### ! Important:

The switch does not support the advertisement of IPv6 addresses to IP phones.

### Procedure steps

- From the navigation tree, double-click **Edit**.
- In the Edit tree, double-click **Diagnostics**.
- In the Diagnostics tree, double-click **802.1AB**.
- In the 802.1AB tree, click **Vendor Specific**.
- In the work area, click the **Local File Servers** tab.
- To select a port, click the **FileServerNum**.
- In the port row, double-click the cell in the **FileServerAddress** column.
- Type an IP address in the box.
- On the toolbar, click **Apply**.

### Field Descriptions

Name	Description
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Defines file server IP address to advertise.



## View the Switch File Server IP Address TLV Configuration using EDM

Use this procedure to display information about the defined local file server IP addresses that switch ports can advertise to IP phones.

### Important:

The switch does not support the advertisement of IPv6 addresses to IP phones.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Local File Servers** tab.

### Field Descriptions

Name	Description
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Displays the defined file server IP address.

## View IP Phone Power Level TLV Information using EDM

Use this procedure to display power level information received on switch ports from an IP phone.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Neighbor Devices** tab.

### Field Descriptions

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected IP phone.

*Table continues...*

Name	Description
CurrentConsLevel	Displays the PoE conservation level configured on the IP phone connected to the switch port.
TypicalPower	Displays the average power level used by the IP phone connected to the switch port.
MaxPower	Displays the maximum power level for the IP phone connected to the switch port.

## View Remote Call Server IP Address TLV Information using EDM

### Procedure steps

Use this procedure to display call server IP address information received on switch ports from an IP phone.

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Neighbor Call Servers** tab.

### Field Descriptions

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected IP phone.
PortCallServerAddressType	Displays the call server IP address type used by the IP phone connected to the switch port.
PortCallServerAddress	Displays the call server IP address used by the IP phone connected to the switch port.

## View Remote File Server IP Address TLV Information using EDM

Use this procedure to display file server IP address information received on switch ports from an IP phone.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.

3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Neighbor File Servers** tab.

### Field Descriptions

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected IP phone.
PortFileServerAddressType	Displays the file server IP address type used by the IP phone connected to the switch port.
PortFileServerAddress	Displays the file server IP address used by the IP phone connected to the switch port.

## View Remote 802.1Q Framing TLV information using EDM

Use this procedure to display Layer 2 frame tagging mode information received on switch ports from connected IP phones.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Neighbor Dot1Q** tab.

### Field Descriptions

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected IP phone.
Dot1QFraming	Displays the Layer 2 frame tagging mode for the IP phone connected to the switch port. Values include: <ul style="list-style-type: none"> <li>• tagged—frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV.</li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• non-tagged—frames are not tagged with 802.1Q priority.</li> <li>• auto—an attempt is made to tag frames based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged.</li> <li>• The default tagging mode is auto.</li> </ul>

## View Remote IP TLV Information using EDM

Use this procedure to display IP address configuration information received on switch ports from connected IP phones.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Neighbor IP Phone** tab.

### Field Descriptions

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected IP phone.
PortPhoneAddressType	Displays the IP address type for the IP phone connected to the switch port.
PortPhoneAddress	Displays the IP address for the IP phone connected to the switch port.
PortPhoneAddressMask	Displays the IP address subnet mask for the IP phone connected to the switch port.
PortPhoneGatewayAddress	Displays gateway the IP address for the IP phone connected to the switch port.

## Configuring Global Energy Saver using EDM

Use the information in this section to configure Energy Saver for an single switch or a stack.

## Enable Global Energy Saver using EDM

Use the following procedure to enable energy saving for the switch.

### Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **EnergySaverEnabled** check box.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

### Energy Saver Globals Tab Field Descriptions

Use the data in the following table to use the **Energy Saver Globals** tab fields.

Name	Description
EnergySaverEnabled	Enables or disables energy saving for the switch.
PoePowerSavingEnabled	Enables or disables Energy Saver PoE power save mode for the switch.
EfficiencyModeEnabled	Enables or disables Energy Saver efficiency mode for the switch.
EnergySaverActive	Activates or deactivates the Energy Saver.

## Disable Global Energy Saver using EDM

Use the following procedure to disable energy saving for the switch.

### Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **EnergySaverEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

## Enable Global Energy Saver PoE Power Save Mode using EDM

Use the following procedure to enable Energy Saver PoE power save mode for the switch.

When enabled, Energy Saver PoE power save mode provides the capability to control power consumption savings for only ports that have Energy Saver enabled, and PoE priority configured to low.

## Prerequisites

- Disable Energy Saver globally.

## Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **PoePowerSavingEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

## Disable Global Energy Saver PoE Power Save Mode using EDM

Use the following procedure to disable Energy Saver PoE power save mode for the switch.

When enabled, Energy Saver PoE power save mode provides the capability to control power consumption savings for only ports that have Energy Saver enabled, and PoE priority configured to low.

## Prerequisites

- Disable Energy Saver globally.

## Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **PoePowerSavingEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

## Enable Energy Saver Efficiency Mode using EDM

Use the following procedure to enable Energy Saver efficiency mode for the switch.

When enabled, Energy Saver efficiency mode enables Energy Saver globally and for each port, enables Energy Saver PoE power save mode, and configures Energy Saver scheduling to predetermined values (on time 18:00 and off time 07:30 daily).

### **Important:**

Energy Saver efficiency mode overrides custom Energy Saver scheduling and PoE power saving mode. You will be prompted to confirm that you want to enable Energy Saver efficiency mode before proceeding.

## Prerequisites

- Disable Energy Saver globally.

## Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **EfficiencyModeEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

## Disable Energy Saver Efficiency Mode using EDM

Use the following procedure to disable Energy Saver efficiency mode for the switch.

When enabled, Energy Saver efficiency mode enables Energy Saver globally and for each port, enables Energy Saver PoE power save mode, and configures Energy Saver scheduling to predetermined values (on time 18:00 and off time 07:30 daily).

## Prerequisites

- Disable Energy Saver globally.

## Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **EfficiencyModeEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

---

## Configuring Energy Saver schedule using EDM

Use the information in this section to configure a time interval for the switch to enter lower power states.

## Configure the Energy Saver Schedule on-time using EDM

Use the following procedure to configure the start of a time interval for the switch to enter lower power states. The time interval can span a complete week, a complete weekend, multiple days, or be configured within an individual day.

## Prerequisites

- Disable Energy Saver globally.

## Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Schedules** tab.
4. Click **Insert**.
5. To choose a day for the Energy Saver schedule on time, select a radio button in the **ScheduleDay** section.
6. To choose an hour of the day for the Energy Saver schedule on time, type a value in the **ScheduleHour** section.
7. To choose a portion of an hour for the Energy Saver schedule on time, type a value in the **ScheduleMinute** section.
8. To configure the selected day, hour, and minutes as the Energy Saver schedule on time, select the **activate** radio button in the ScheduleAction section.

Activate is selected by default.

9. Click **Insert**.

## Field Descriptions

The following table describes the fields of Insert Energy Saver Schedule screen.

Name	Description
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.

## Configure the Energy Saver Schedule off time using EDM

Use the following procedure to configure the end of a time interval for the switch to enter lower power states. The time interval can span a complete week, a complete weekend, multiple days, or be configured within an individual day.

## Prerequisites

- Disable Energy Saver globally.

## Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Schedules** tab.



4. Click **Insert**.
5. To choose a day for the Energy Saver schedule off time, select a radio button in the **ScheduleDay** section.
6. To choose an hour of the day for the Energy Saver schedule off time, type a value in the **ScheduleHour** section.
7. To choose a portion of an hour for the Energy Saver schedule off time, type a value in the **ScheduleMinute** section.
8. To configure the selected day, hour, and minutes as the Energy Saver schedule off time, select the **deactivate** radio button in the ScheduleAction section.  
Activate is selected by default.
9. Click **Insert**.

## Modify an Energy Saver Schedule on and off time Status using EDM

Use the following procedure to change an existing schedule off time to on time or to change an existing schedule on time to off time.

### Prerequisites

- Disable Energy Saver globally.

### Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **Energy Saver**.
3. In the work area, click the **Energy Saver Schedules** tab.
4. To select a schedule time to edit, click a schedule day.
5. In the schedule day 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**.

---

## Configuring Port-based Energy Saver using EDM

Configure port-based Energy Saver to enable or disable energy saving for individual ports, or all ports on a switch or stack.

### Configure Energy Saver on Individual Ports

Use the following procedure to enable or disable Energy Saver for individual ports on a switch or stack.

## Procedure

1. Follow one of the following paths:
  - From the **Device Physical View**, select a port, or use Ctrl-click to select more than one port, then follow the navigation tree to **Edit > Chassis > Ports > Energy Saver** tab.
  - From the navigation tree, go to **Power Management > Energy Saver > Ports** tab.
2. In the Port row, double-click the cell in the **EnergySaverEnabled** column.
3. Select **true** from the drop-down list to enable Energy Saver, or **false** to disable Energy Saver for the port.
4. Repeat the above steps for additional ports.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

## Ports Tab Field Descriptions

The following table describes the fields of **Ports** tab.

Name	Description
Port	Indicates the port.
EnergySaverEnabled	Indicates whether the Energy Saver feature is enabled for the port.
EnergySaverPoeStatus	A read-only cell. Values include: <ul style="list-style-type: none"> <li>• enabled</li> <li>• disabled</li> <li>• notApplicable</li> </ul>

## Viewing Energy Saver 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, click **Energy Saver**.
3. In the work area, click the **Energy Savings** tab.
4. On the toolbar, you can click **Refresh** update the data.

### Field Descriptions

Use the data in this table to help you understand the displayed Energy Saver information.

Name	Description
Total	Indicates the total power saving values for all switches in a stack.
UnitIndex	Indicates the unit number of the switch.
UnitSavings(watts)	Indicates the total power capacity being saved on the switch.
PoeSavings(watts)	Indicates the total PoE power being saved on the switch.

# Chapter 4: Network Time Protocol

This chapter describes the Network Time Protocol (NTP).

---

## NTP Fundamentals

The Network Time Protocol (NTP) synchronizes the internal clocks of various network devices across large, diverse networks to universal standard time. NTP runs over the User Datagram Protocol (UDP), which in turn runs over IP.

NTPv4 is the current protocol version, which is documented in Request For Comments (RFC) 5905 and is backward compatible with version 3, specified in RFC 1305. NTPv4 supports IPv4 and IPv6.

**\* Note:**

Synchronization to the NTP server using NTP sync-now functionality is not supported. With NTPv4, the synchronization to the NTP server takes place continuously by exchange of requests and updates so that the sync-now functionality is not needed.

Every network device relies on an internal system clock to maintain accurate time. On local devices, the internal system clock is usually set by eye or by a wristwatch to within a minute or two of the actual time and is rarely reset at regular intervals. Many local clocks are battery-backed devices that use room temperature clock oscillators that can drift as much as several seconds each day. Network Time Protocol solves this problem by automatically adjusting the time of the devices so that they are synchronized within a millisecond (ms) on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time (UTC).

The current implementation of NTP supports only unicast client mode. In this mode, the NTP client sends NTP time requests to other remote time servers in an asynchronous fashion. The NTP client collects four samples of time from each remote time server. A clock selection algorithm determines the best server among the selected samples based on stratum, delay, dispersion and the last updated time of the remote server.

The System Clock is adjusted to the selected sample from the chosen server.

---

## NTP terms

A peer is a device that runs NTP software. However, this implementation of NTP refers to peers as remote time servers that provide time information to other time servers on the network and to the local NTP client. An NTP client refers to the local network device, a switch which accepts time information from other remote time servers.

---

## NTP system implementation model

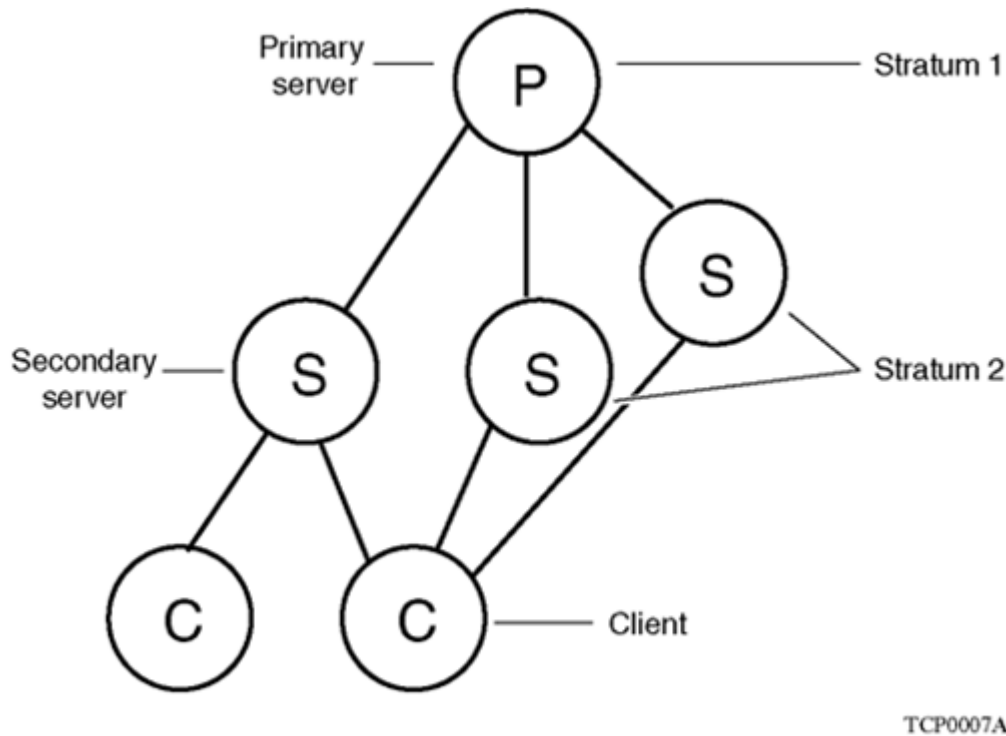
NTP is based on a hierarchical model that consists of a local NTP client that runs on the switch and on remote time servers. The NTP client requests and receives time information from one or more remote time servers. The local NTP client reviews the time information from all available time servers and synchronizes its internal clock to the time server whose time is most accurate. The NTP client does not forward time information to other devices running NTP.

Two types of time servers exist in the NTP model: primary time servers and secondary time servers. A primary time server is directly synchronized to a primary reference source, usually a wire or radio clock that is synchronized to a radio station providing a standard time service.

The primary time server is the authoritative time source in the hierarchy, meaning that it is the one true time source to which the other NTP devices in the subnet synchronize their internal clocks.

A secondary time server uses a primary time server or one or more secondary time servers to synchronize its time, forming a synchronization subnet. A synchronization subnet is a self-organizing, hierarchical master-slave configuration with the primary servers at the root and secondary servers of decreasing accuracy at successive levels.

The following figure shows NTP time servers forming a synchronization subnet.



**Figure 11: NTP time servers forming a synchronization subnet**

In the NTP model, the synchronization subnet automatically reconfigures in a hierarchical primary-secondary (master-slave) configuration to produce accurate and reliable time, even if one or more primary time servers or the path between them fails. This feature applies where all the primary servers on a partitioned subnet fail, but one or more backup primary servers continue to operate. If all of the primary time servers in the subnet fail, the remaining secondary servers synchronize among themselves.

## Time distribution within a subnet

NTP distributes time through a hierarchy of primary and secondary servers, with each server adopting a stratum. A stratum defines how many NTP hops away a particular secondary time server is from an authoritative time source (primary time server) in the synchronization subnet. A stratum 1 time server is located at the top of the hierarchy and is directly attached to an external time source, typically a wire or radio clock; a stratum 2 time server receives its time through NTP from a stratum 1 time server; a stratum 3 time server receives its time through NTP from a stratum 2 time server, and so forth.

Each NTP client in the synchronization subnet chooses as its time source the server with the lowest stratum number with which it is configured to communicate through NTP. This strategy effectively builds a self-organizing tree of NTP speakers. The number of strata is limited to 15 to avoid long synchronization loops.

NTP avoids synchronizing to a remote time server whose time is inaccurate. NTP never synchronizes to a remote time server that is not itself synchronized. NTP compares the times reported by several remote time servers.

---

## Synchronization

Unlike other time synchronization protocols, NTP does not attempt to synchronize the internal clocks of the remote time servers to each other. Rather, NTP synchronizes the clocks to universal standard time, using the best available time source and transmission paths to that time source.

NTP uses the following criteria to determine the time server whose time is best:

- The time server with the lowest stratum.
- The time server closest in proximity to the primary time server (reduces network delays).
- The time server offering the highest claimed precision.

NTP accesses several (at least three) servers at the lower stratum level because it can apply an agreement algorithm to detect a problem on the time source.

---

## NTP modes of operation

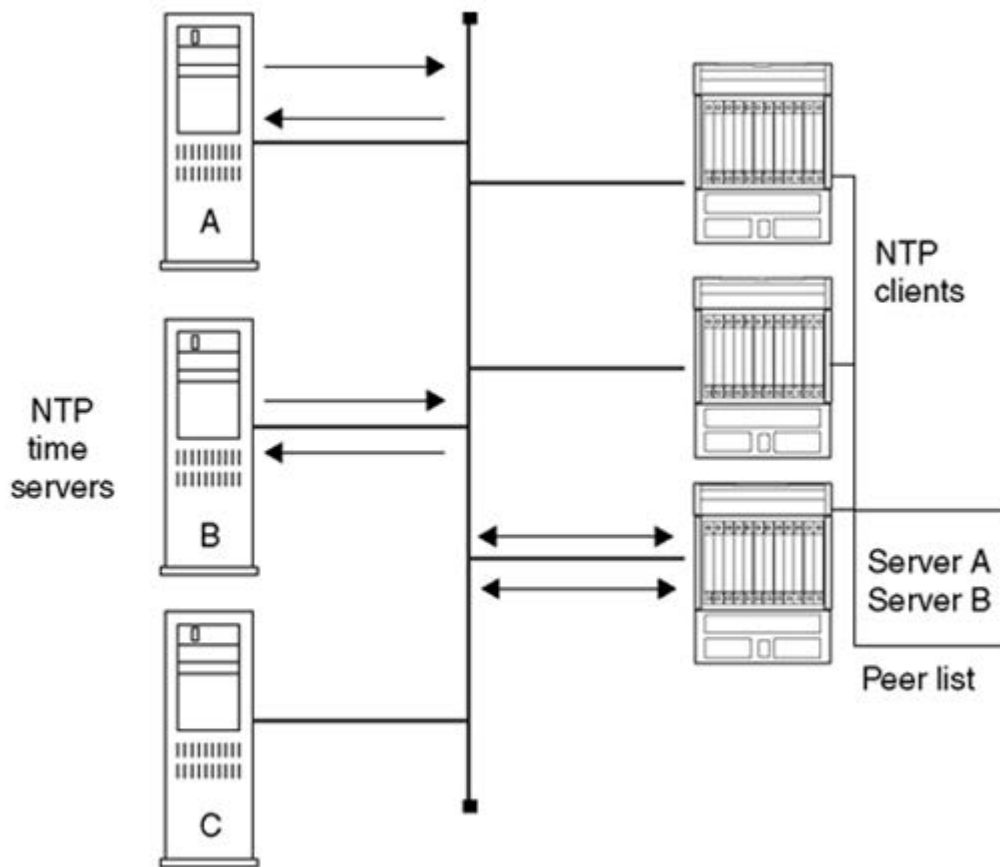
NTP uses unicast client mode to enable time servers and NTP clients to communicate in the synchronization subnet. The switch supports only unicast client mode.

After you configure a set of remote time servers (peers), NTP creates a list that includes each time server IP address. The NTP client uses this list to determine the remote time servers to query for time information.

After the NTP client queries the remote time servers, the servers respond with various timestamps, along with information about their clocks, such as stratum, precision, and time reference.

The NTP client reviews the list of responses from all available servers and chooses one as the best available time source from which to synchronize its internal clock.

The following figure shows how NTP time servers operate in unicast mode.



TCP0006A

Figure 12: NTP time servers operating in unicast client mode

## NTP Authentication

You can authenticate time synchronization to ensure that the local time server obtains its time services only from known sources. NTP authentication adds a level of security to your NTP configuration. By default, network time synchronization is not authenticated.

If you select authentication, the switch uses the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA1) to produce a message digest of the key. The message digest is created using the key and the message, but the key itself is not sent. The MD5 or SHA1 algorithms verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

To authenticate the message, the client authentication key must match that of the time server. Therefore, the authentication key must be securely distributed in advance (the client administrator must obtain the key from the server administrator and configure it on the client).



While a server can know many keys (identified by many key IDs) it is possible to declare only a subset of these as trusted. The time server uses this feature to share keys with a client that requires authenticated time and that trusts the server, but that is not trusted by the time server.

---

## Configuring NTP using the CLI

Use these procedures to configure the Network Time Protocol (NTP) using the Command Line Interface (CLI). Perform the procedures in the order they are provided.

---

### Prerequisites to NTP Configuration

Unless otherwise stated, to perform the procedures in this section, you must log on to the Global Configuration mode in the CLI. For more information about using CLI, see [Using CLI and EDM on Ethernet Routing Switch 4900 and 5900 Series](#).

Before you configure NTP, you must perform the following task:

Configure an IP interface on the switch and ensure that the NTP server is reachable through this interface. For instructions, see [Configuring IP Routing and Multicast on Ethernet Routing Switch 4900 and 5900 Series](#).

**!** **Important:**

NTP server MD5 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

---

### NTP configuration procedures

Use the task flow shown in the following figure to determine the sequence of procedures to perform to configure NTP.

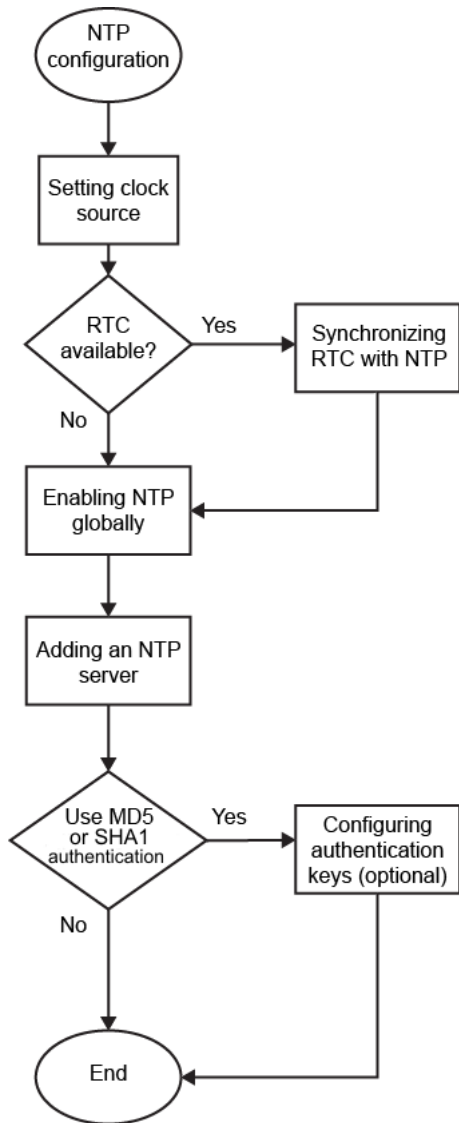


Figure 13: NTP configuration procedures in CLI

## Configuring System Clock

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

You can perform clock tasks such as setting the default clock source, synchronizing the clock with SNTP, disabling the clock and SNTP synchronization, or resetting the clock synchronization to default.

### Set the default Clock Source

#### About this task

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

The default clock source is SNTP.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `clock source` command.

Variable	Definition
clock source {ntp   sntp   rtc   sysUpTime}	Sets the clock source as one of: <ul style="list-style-type: none"> <li>• Network Time Protocol (ntp)</li> <li>• Simple Network Time Protocol (sntp)</li> <li>• Real Time Clock (rtc)</li> <li>• System Up Time (sysUpTime)</li> </ul> The default clock source is SNTP.

## Synchronize the Real Time Clock

### Before you begin

SNTP must be enabled.

### About this task

Use this procedure to synchronize RTC with SNTP/NTP.

By default, RTC is not synchronized with either NTP or SNTP. SNTP/NTP synchronization can be configured.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable clock synchronization:

```
[no] [default] clock sync-rtc-with-time-client enable
```

## Synchronize Real Time Clock

By default, Real Time Clock (RTC) is not synchronized with either NTP or SNTP. SNTP/NTP synchronization can be configured.

### About this task

Use this procedure to synchronize RTC with SNTP or NTP.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
[no] [default] clock sync-rtc-with-time-client enable
```

3. Press Enter.

### Variable Definitions

Use the data in the following table to use the `clock` command.

Variable	Definition
enable	Activates or disables RTC synchronization.
syncn-rtc-with-time-client	Configures RTC synchronization with NTP/SNTP status.

---

## Enable NTP Globally

### About this task

Use this procedure to enable NTP globally.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
[no] ntp
```

3. Press Enter.

### Variable definitions

Use the data in the following table to use the `ntp` command.

## Variable definition

Variable	Value
no	Disables NTP globally.
default	Resets NTP globally to default value.

## Create Authentication Keys

### About this task

Use this procedure to create authentication keys for MD5 or SHA1 authentication. You can create a maximum of 10 keys.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
[no] [default] ntp authentication-key <1-65535> type [ md5 | sha1 ]
<word>
```

3. Press Enter.

### Example

The following is an example of authentication key creation:

1. Create the authentication key:

```
Switch(config)# ntp authentication-key 5 type sha1 test
```

2. Enable MD5 authentication for the NTP server:

```
Switch(config)# ntp server 47.140.53.187 auth-enable
```

3. Assign an authentication key to the NTP server:

```
Switch(config)# ntp server 47.140.53.187 authentication-key 5
```

## Variable definitions

Use the data in the following table to use the `ntp authentication-key` command.

Variable	Definition
<1-65535>	Creates an authentication key for MD5/SHA1 authentication.
no	Disables all NTP authentication keys.
default	Returns NTP authentication keys to the default value.
type	Specifies the authentication method: md5 or sha1.
<word>	Specifies the secret key. Maximum 20 characters.

---

## Configure an NTP Server

### About this task

Use this procedure to add or delete an NTP server. You can configure a maximum of 10 NTP servers.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
[no] [default] ntp server {<A.B.C.D> | <IPv6_address>}
```

3. Press Enter.

## Variable Definitions

Use the data in the following table to use the `ntp server` command.

Variable	Definition
<A.B.C.D>	Specifies the IPv4 address of the NTP server.
<IPv6_address>	Specifies the IPv6 address of the NTP server.
no	Deletes the NTP server.
default	Resets the NTP server to the default. DEFAULT: Not enabled, No Authentication, No Authentication keys

---

## Modify Options for an NTP Server

### About this task

Use this procedure to modify the existing options for an NTP server that is identified by its IP address.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
[default] [no] ntp server {<A.B.C.D.> | <IPv6_address>} [auth-
enable] [authentication-key <1-65535>] [enable]
```

3. Press Enter.

### Example

```
Switch(config)# ntp server 47.140.53.187
```

## Variable Definitions

Use the data in the following table to use the `ntp server` command.

Variable	Definition
auth-enable	Activates MD5 or SHA1 authentication on this NTP server. DEFAULT: no authentication To set this option to the default value, use the default operator with the command.
<A.B.C.D>	Specifies the IPv4 address of the NTP server.
<IPv6_address>	Specifies the IPv6 address of the NTP server.
authentication-key <1-65535>	Specifies the key ID value used to generate the MD5 or SHA1 digest for the NTP server in the range of 1 to 65535. If this parameter is omitted, the key defaults to 0 (disabled authentication). To set this option to the default value, use the default operator with the command.
default	Sets the NTP server to the default. DEFAULT: No authentication. Disabled authentication.
no	Deletes the NTP server.

## Display NTP Settings

### About this task

Use this procedure to view the NTP key, NTP server settings, and NTP statistics.

### Procedure

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

```
show ntp [key] [server] [statistics]
```

3. Press Enter.

### Example

```
Switch#show ntp
NTP client enabled      : true
Last NTP update        : MON AUG 07 15:53:45 2017 UTC
Sync state              : synchronized to 192.0.2.1 (stratum 1)
Switch#show ntp
```

## Network Time Protocol

```
Key ID Key
1 test 1
1911      test 2

Switch#show ntp server

Server IP          Enabled      Auth      Key ID
192.0.2.10         true        true      1911
Switch#show ntp statistics

-----
NTP Server : 192.0.2.10
-----
      Stratum : 5
      Version : 2
      Sync Status : synchronized
      Reachability : reachable
      Root Delay : 0.190536547
      Precision : 0.00003051
      Access Attempts : 1
      Server Fail : 0
```

## Variable definitions

Use the data in the following table to use the `show ntp` command.

Variable	Definition
server	Display NTP server information.
key	Display NTP authentication keys.
statistics	Displays information about the status of the NTP server: <ul style="list-style-type: none"><li>• Number of NTP requests sent to this NTP server</li><li>• Number of times this NTP server updated the time</li><li>• Number of times this NTP server was rejected attempting to update the time</li><li>• Stratum</li><li>• Version</li><li>• Sync Status</li><li>• Reachability</li><li>• Root Delay</li><li>• Precision</li></ul>

---

## Configuring NTP using the EDM

This section describes how to configure the Network Time Protocol (NTP) using Enterprise Device Manager.



## Configuring NTP using the EDM

### Prerequisites

Before you configure NTP, you must perform the following tasks:

- Configure an IP interface on the switch and ensure that the NTP server is reachable through this interface. For instructions, see [Configuring IP Routing and Multicast on Ethernet Routing Switch 4900 and 5900 Series](#).

### ! Important:

NTP server MD5/SHA1 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

## Enable NTP Globally using EDM

### Prerequisites

Before you configure NTP, you must perform the following tasks:

- Configure an IP interface on the switch and ensure that the NTP server is reachable through this interface. For instructions, see [Configuring IP Routing and Multicast on Ethernet Routing Switch 4900 and 5900 Series](#).

### ! Important:

NTP server MD5/SHA1 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

Use this procedure to enable NTP globally on the switch. Default values are in effect for most NTP parameters.

### ! Important:

If NTP is already activated, this configuration does not take effect until you disable NTP, and then re-enable it.

### Procedure steps

1. From the navigation tree, click **Edit**.
2. In the Edit tree, click **NTP**.
3. On the **Globals** tab, select the **Enable** check box.
4. Click **Apply**.

## Globals Tab Field Descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
Enable	Activates or disables NTP.

Name	Description
	DEFAULT: NTP is disabled.

## Add or Remove an NTP Server using EDM

### Prerequisites

Before you configure NTP, you must perform the following tasks:

- Configure an IP interface on the switch and ensure that the NTP server is reachable through this interface. For instructions, see [Configuring IP Routing and Multicast on Ethernet Routing Switch 4900 and 5900 Series](#).

Use this procedure to add or remove a remote NTP server to the configuration by specifying its IP address. NTP adds this IP address to a list of servers, which the local NTP client uses when it queries remote time servers for time information. The list of qualified servers called to as a peer list. You can configure a maximum of 10 NTP servers.

### Procedure steps

1. From the navigation tree, click **Edit**.
2. In the Edit tree, click **NTP**.
3. Click the **Server** tab.
4. Click **Insert**.
5. Specify the IP address of the NTP server.
6. Click **Insert**.

The IP address of the NTP server that you configured is displayed in the ServerAddress tab of the NTP dialog box.

## Server Tab Field Descriptions

Use the data in the following table to use the **Server** tab.

Name	Description
AddressType	Specifies the type of the IP address.
Address	Specifies the IP address of the remote NTP server.
Enable	Activates or disables the remote NTP server.
Authentication	Activates or disables MD5/ SHA1 authentication on this NTP server. MD5/SHA1 produces a message digest of the key. MD5/SHA1 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.  DEFAULT: no authentication

*Table continues...*

Name	Description
KeyId	Specifies the key ID used to generate the MD5/SHA1 digest for this NTP server within the range of 1 to 65535.  * <b>Note:</b> If MD5/SHA1 authentication is activated, the key ID must be previously configured. If authentication is disabled, this field is not used. If this field is left blank, the key ID displays a value of 0.
AccessAttempts	Specifies the number of NTP requests sent to this NTP server.
AccessSuccess	Specifies the number of times this NTP server updated the time.
AccessFailure	Specifies the number of times this NTP server was rejected while attempting to update the time.
Stratum	This variable is the stratum of the server.
Version	This variable is the NTP version of the server.
RootDelay	This variable is the root delay of the server.
Precision	This variable is the NTP precision of the server in seconds.
Reachable	This variable is the NTP reach ability of the server.
Synchronized	This variable is the status of synchronization with the server.

## Configure Authentication Keys using EDM

### Prerequisites

Before you configure NTP, you must perform the following tasks:

- Configure an IP interface on the switch and ensure that the NTP server is reachable through this interface. For instructions, see [Configuring IP Routing and Multicast on Ethernet Routing Switch 4900 and 5900 Series](#).

Use this procedure to assign an NTP key to use MD5 or SHA1 authentication on the server.

### Procedure steps


1. From the navigation tree, click **Edit**.
2. In the Edit tree, click **NTP**.
3. Click the **Key** tab.
4. Click **Insert**.
5. Insert the key ID and the MD5 key ID or SHA1 key ID in the Insert Key dialog box.

6. Click **Insert**.

The values that you specified for the key ID and the MD5 key ID or SHA1 key ID are displayed in the Key tab of the NTP dialog box.

## Key Tab Field Descriptions

Use the data in the following table to use the **Key** tab.

Name	Description
KeyId	<p>Specifies the key id used to generate the MD5/SHA1 digest within a range of 1 to 65535.</p> <p>You can enter the public key in the Insert Key dialog box. You cannot edit the public key on the Key tab directly.</p>
KeySecret	<p>This field is the MD5/SHA1 key used to generate the MD5/SHA1 digest. The key can be an alphanumeric string between 0 and 20.</p> <p> <b>Note:</b></p> <p>You cannot specify the number sign (#) as a value in the KeySecret field. The NTP server interprets the # as the beginning of a comment and truncates all text entered after the #. This limitation applies to xntpd, the NTP daemon, version 3 or lower.</p>

# Chapter 5: Power over Ethernet

Power over Ethernet (PoE) in the ERS 4900 and 5900 Series provide IEEE 802.3at-compliant power or PoE+ on all 10/100/1000 RJ-45 ports. The uPOE model, ERS 5928GTS-uPWR supports 60W.

The PoE+ capable devices can deliver between 3 and 32 watts and the uPOE model, ERS 5928GTS-uPWR can deliver up to 60 watts. These devices have the added ability to detect IEEE 802.3at and legacy devices.

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

Power over Ethernet (uPOE) is for emerging IoT deployments such as smart lighting, medical systems and high-end video surveillance

For more information about power supplies, see [Installing Ethernet Routing Switch 4900 Series](#) and [Installing Ethernet Routing Switch 5900 Series](#).

You can configure PoE from the Command Line Interface (CLI), Enterprise Device Manager (EDM), and SNMP.

---

## Power over Ethernet Fundamentals

This section provides conceptual information related to the configuration and management of Power over Ethernet (PoE).

---

### PoE Overview

The ERS 5900 PWR+ models (ERS 59100GTS-PWR+, ERS 5928GTS-PWR+ and ERS 5952GTS-PWR+) and ERS 4900 PWR+ models (ERS 4926GTS-PWR+ and ERS 4950GTS-PWR+) are ideal to use with IP phones, hubs, and wireless access points. The ERS 5928GTS-uPWR and ERS 5928MTS-uPWR are ideal to use for emerging IoT deployments, such as smart lighting, medical systems, and high-end video surveillance. You can use these switches with all network devices.

By using the switch series PWR+ units, you can plug any IEEE802.3at-compliant powered device into a front-panel port and receive power in that port. Data also can pass simultaneously on that port. This capability is called PoE.

For more information about PoE and power supplies, see [Installing Ethernet Routing Switch 5900 Series](#).

The ERS 5900 and ERS 4900 PWR+ models automatically detect any IEEE 802.3at-compliant powered device attached to any PoE front panel port and immediately send power to that appliance. UPoE capable ports support 802.1af and 802.1at capable powered devices, and UPoE capable devices that have 2 two-pair circuits, where each two-pair circuit operates as an 802.1at capable powered device.

The power detection function of the switch series PWR+ models, operate independent of the data link status. A device that is already operating the link for data or a device that is not yet operational can request power. That is, the switches provide power to a requesting device even if the data link for that port is disabled. The switches monitor the connection and automatically disconnect power from a port when you remove or change the device, as well as when a short circuit occurs.

The switches automatically detect devices that require no power connections from them, such as laptop computers or other switching devices, and sends no power to those devices. You control the supply of power to specific ports by setting the maximum allowed power to each port in 1 watt increments, from 3 watts to 32 watts for PWR+ models and 60 watts for uPoE model.

**!** **Important:**

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

The Data Link Layer (DLL) classification provides finer power resolution and the ability for Power Sourcing Equipment (PSE) and Powered Device (PD) to participate in dynamic power allocation. This ability is enabled by configuring the PoE PD detection type (802.3at or 802.3at\_and\_legacy) to support a DLL classification for communication.

The PWR+ devices support the IEEE 802.3at-2009 standard for an Link Layer Discovery Protocol (LLDP) configuration with a PD. The LLDP support for PoE+ is added by extending the existing standard LLDP DOT3 Power through MDI TLV defined by the IEEE 802.1ab with the new fields and values defined in the IEEE 802.3at-2009 standard.

For more information, see [LLDP support for PoE+](#) on page 343.

**\*** **Note:**

The LLDP support for the PoE+ feature is available only on the PWR+ models.

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

---

## PoE high inrush mode

Some non-standard Powered Devices (PD) require more than 15W at power up. For such devices, the power up mode can be configured to high inrush on the specific port that the PD connects to.

---

## PoE Power Priority and Limit for IP Phones

The switch allows the provisioning of PoE priority levels and power limits when an IP Phone is discovered. Before connecting any phone to the switch, you have the option to configure two global PoE variables: the IP Phone port power limit and the IP Phone port power priority. After the switch detects an IP Phone, the PoE priority and the power limit settings are configured dynamically with the predefined values (if present). The dynamic settings are applied regardless of the discovery mechanism for IP Phones (ADAC, 802.1ab, 802.1x or any other future discovery mechanism). The dynamic settings are not applied without a proper configured IP Phone discovery method.

You can configure the power limit for the IP Phone in the range of 3 to 32 watts.. The actual power allocated, however, is limited by the power available from the system power pool.

Once the system applies the IP Phone dynamic values, they are read-only until the IP Phone disconnects from the supplying power port. You can change the global IP Phone settings for the next IP Phone connection or the PoE settings of the port for the next consuming power device. The port settings are kept, even if they are not applied, while an IP Phone is connected on the particular port.

### **Note:**

The dynamic values of IP Phone power priority and power limit per port are available only if an IP Phone is connected on the port. When the IP Phone disconnects, the PoE port power priority and power limit return to previously-configured values.

---

## LLDP support for PoE+

LLDP is a link (point-to-point) MAC protocol which is used to allow switches and routers to automatically discover a network topology. Under IEEE 802.3at, LLDP is extended to perform a link configuration function related to power negotiation between a PSE and PD.

The DLL scheme uses a PoE-specific LLDP specified in the Clause 79 (IEEE 802.3) with additional protocol rules defined in Clause 33 (IEEE 802.3at). According to Clause 33, there are two power entities, PD and PSE. These entities allow devices to draw or supply power over the sample generic cabling as used for data transmission.

You can configure the PoE PD detection type (802.3at or 802.3at\_and\_legacy) to support a DLL classification for communication. The Data Link Layer classification provides finer power resolution and the ability for PSE and PD to participate in dynamic power allocation. The allocated power to the PD can change one or more times during PD operation.

The following configurations must be enabled on a PoE-capable port for applying LLDP support for PoE+:

- Link Layer Discovery Protocol Data Units (LLDPDUs) for transmission and reception
- Power-via-MDI TLV transmit flag
- PD detection type must be 802.3at or 802.3at\_and\_legacy

By default, the LLDPDU transmission and reception are enabled on all device under test (DUT) ports.

For more information about the power through MDI TLV, see [802](#) on page 370.

### Class PoE Management Mode

In class PoE management mode, the maximum power for an interface is determined by the class of the connected powered device.

The following table lists the classes of powered devices and associated power levels.

Standard	Class	Maximum power delivered by PoE port	Power range of powered device
IEEE 802.3af (PoE) and IEEE 802.3at (PoE+)	0	15.4 watts	0.44 through 12.95 watts
	1	4.0 watts	0.44 through 3.84 watts
	2	7.0 watts	3.84 through 6.49 watts
	3	15.4 watts	6.49 through 12.95 watts
IEEE 802.3at (PoE+)	4	30.0 watts	12.95 through 25.5 watts
uPoE	4	60.0 watts	25.5 through 55.5 watts

Due to line loss, the power range of the PD is less than the maximum power delivered at the PoE port for each class. Line loss is influenced by cable length, quality, and other factors and is typically around 10 to 25 percent.

The powered device communicates to the PoE controller which class it belongs to when it is connected. The PoE controller then allocates to the interface the maximum power required by the class. It does not allocate power to an interface until a powered device is connected. Class 0 is the default class for powered devices that do not provide class information. Class 4 powered devices are supported only by PoE ports that support IEEE 802.3at (PoE+) and uPoE.

The default detection type for PWR+ models is 802.3at\_and\_legacy.

---

## Port power priority

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

The switch automatically drops low-priority ports when the power requirements exceed the available power budget. When the power requirements becomes lower than the switch power budget, the power returns to the dropped port. When several ports have the same priority and the power budget is exceeded, the ports with the highest interface number are dropped until the consumption is within the power budget.



For example, assume the following scenario:

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

The devices connected to the ports consume the available switch power. The device connected to port 41 requests power from the switch. The switch provides the required power, as port 41 is configured as high priority. However, to maintain the power budget, the switch powers off one of the ports configured as low priority. In this case, the switch powers off port 40 and provides power to port 41. If another port drops power, the system automatically reinstates power to port 40.

---

## Configuring Power over Ethernet using the CLI

The following sections provide procedures to configure Power over Ethernet (PoE) using the CLI.

---

### Enable Port Power

#### About this task

Use this procedure to enable PoE to a port.

#### Procedure


1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
poe poe-shutdown [port <portlist>]
```
3. Press Enter.

### Variable Definitions

Use the data in the following table to use the `poe poe-shutdown` command.

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

---

## Disable Port Power

### About this task

Use this procedure to disable PoE to a port.

### Procedure


1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
no poe-shutdown [port <portlist>]
```
3. Press Enter.

## Variable Definitions

Use the data in the following table to use the `no poe-shutdown` command.

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

---

## Set Port Power Priority

### About this task

Use this procedure to set the port power priority.

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
poe poe-priority [port <portlist>] {critical | high | low}
```
3. Press Enter.

## Variable Definitions

Use the data in the following table to use the `poe poe-priority` command.

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

## Set Power Limit for Channels

### About this task

Use this procedure to set the power limit for channels.

### Procedure

1. Enter Ethernet Interface Configuration mode:  

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:  

```
po e poe-limit [port <portlist>] <3-32> <3-60>
```
3. Press Enter.

## Variable Definitions

Use the data in the following table to use the `po e poe-limit` command.

Variable	Definition
<portlist>	Specifies the ports for which to set the limit.  * <b>Note:</b> If you omit this parameter, the system uses the port number you specified in the interface command.
<3-32>	Specifies the power range limit for PoE+ units, from 3 to 32 Watts.
<3-60>	Specifies the power range limit for PoE+ units, from 3 to 60 Watts.

## Configure PoE Power Up Mode

**About this task**

To allow non-standard Powered Devices (PD) to draw power from PoE switches by configuring the port power up mode.

**Procedure**

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

2. Configure the PoE power up mode:

**Display PoE Main Configuration****About this task**

Use this procedure to display the main PoE configuration.

**Procedure**

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show poe-main-status [unit <1-8>]
```

3. Press Enter.

**Variable definitions**

Use the data in the following table to use the `show poe-main-status` command.

Variable	Definition
unit <1-8>	Displays main PoE configuration for the specified unit in the stack.

**Set a Power Usage Threshold****About this task**

Use this procedure to set a percentage threshold above which the switch sends a warning trap message.

If the PoE power usage exceeds the threshold and SNMP traps are configured appropriately, the switch sends the `pethMainPowerUsageOnNotification` trap. If the power consumption exceeds and then falls below the threshold, the switch sends the `pethMainPowerUsageOffNotification` trap.

**Procedure**

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
po e poe-power-usage-threshold [unit <1-8>] <1-99>
```

3. Press Enter.

**Variable definitions**

Use the data in the following table to use the `po e poe-power-usage-threshold [unit <1-8>] <1-99>` command.

Variable	Definition
unit <1-8>	Specifies the unit in the stack for which to set the power threshold.
<1-99>	Specifies the percentage of total available power you want the switch to use prior to sending a trap.

**Set the Method to Detect Power Devices****About this task**

Use this procedure to set the method the switch uses to detect the power devices connected to the front ports.

The `po e-pd-detect-type` command enables 802.3at or Legacy compliant PD detection methods for PWR+ units.

**\* Note:**

This setting applies to the entire switch, not port-by-port. You must ensure that this setting is configured correctly for all the IP appliances on a specified switch.

**Procedure**

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
po e poe-pd-detect-type [unit <1-8>] {802dot3at |
802dot3at_and_legacy}
```

3. Press Enter.

## Variable definitions

Use the data in the following table to use the `poe poe-pd-detect-type` command.

Variable	Definition
unit <1-8>	Specifies the unit in the stack to set the detection mode.
802dot3af   802dot3af_and_legacy   802dot3at   802dot3at_and_legacy	Sets the detection method the switch uses to detect power needs of devices connected to the front ports: <ul style="list-style-type: none"> <li>• 802dot3af</li> <li>• 802dot3af_and_legacy</li> <li>• 802dot3at</li> <li>• 802dot3at_and_legacy</li> </ul>

## Display PoE Port Configuration

### About this task

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

### Procedure

1. Enter Privileged EXEC mode:

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

```
show poe-port-status [<portlist>]
```
3. Press Enter.

### Example

```
Switch#show poe-port-status
Unit Admin   Current      Limit      Power-up
Port Status   Status       Class      (Watts)    Priority    Mode
-----
1/1  Enable   Detecting    0  32      Low      802.3af
1/2  Enable   Detecting    0  32      Low      802.3af
1/3  Enable   Detecting    0  32      Low      802.3af
1/4  Enable   Detecting    0  32      Low      802.3af
1/5  Enable   Detecting    0  32      Low      802.3af
1/6  Enable   Detecting    0  32      Low      802.3af
```

## Variable definitions

Use the data in the following table to use the `show poe-port-status` command.

Variable	Definition
<portlist>	Specifies a specific port or list of ports.

---

## Display PoE Power Measurement

### About this task

Use this procedure to display the power configuration.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. At the command prompt, enter the following command:  

```
show poe-power-measurement [<portlist>]
```
3. Press Enter.

### Variable definitions

Use the data in the following table to use the `show poe-power-measurement` command.

Variable	Definition
<portlist>	Specifies the ports for which to display configuration.

---

## Download PoE Firmware from SFTP

Perform the following procedure to download the PoE image file from SFTP.

### Procedure

1. Enter Global Configuration mode:  

```
enable
```

```
configure terminal
```
2. Download the SFTP PoE image file:  

```
download sftp poe_module_image <image_name>
```

---

## Configure PoE Priority for IP Phone

### About this task

Set the PoE priority for the IP Phone and the power limit to the PoE port for power consumption.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

## 2. Configure PoE priority for IP phone.

```
poe ip-phone [poe-limit <3-32>] [poe-priority <low | high |
critical>]
```

### \* Note:

This command is not supported on non-PoE models.

## Variable definitions

Use the information in the following table to set the PoE priority for the IP Phone and the power limit to the PoE port for power consumption.

### Variable definition

Variable	Value
poe-limit <3-32>	The power limit, range is from 3 to 32 W, The maximum for PoE switch models is 16W, and 32W for PoE+ models
Poe-priority <low   high   critical>	The PoE priority for the port.

## Disable PoE Priority and Power Limit

### About this task

Use this procedure to disable the PoE priority and power limit settings.

### Procedure

#### 1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
no poe-ip-phone [poe-limit] [poe-priority]
```

#### 3. Press Enter.

## Variable definitions

Use the data in the following table to use the `no poe-ip-phone` command.

Variable	Definition
poe-limit <3-32>	Specifies the power limit. Range is from 3 to 32 W

*Table continues...*



Variable	Definition
poe-priority {low   high   critical}	Specifies the PoE priority for the port.

## Configuring Power over Ethernet using EDM

The following sections provide procedures to configure and manage Power over Ethernet (PoE) using the EDM.

### View PoE Ports using EDM

The front panel view of Enterprise Device Manager (EDM) provides additional information for PoE ports on the PoE switch. This additional information is in the form of a colored **P** that appears inside the graphic representation of the port. This colored P represents the current power aspect of the PoE port.

[Table 17: Power Aspect color codes](#) on page 353 explains the different colors displayed by the power aspect.

**Table 17: Power Aspect color codes**

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

#### Important:

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

## Managing PoE for a Switch Unit using the EDM

Use this procedure to display and manage PoE for a single switch unit.

### Procedure Steps

1. From the Device Physical View, click a switch unit with PoE ports.
2. From the navigation tree, choose **Edit**.

3. In the Edit tree, double-click **Unit**.
4. In the work area, click the **PoE** tab.
5. In the **UsageThreshold%**, type a value.
6. In the **PowerDeviceDetectType** section, click a radio button.
7. Click **Apply** .

**\* Note:**

You can also display and manage PoE from the navigation tree path **Power Management > PoE > Globals-PoE Units**.

## Field Descriptions

Use the data in the following table to display and manage PoE for a switch unit.

Name	Description
Power(watts)	Displays the total power (in watts) available to the switch.
OperStatus	Displays the power state of the switch: <ul style="list-style-type: none"> <li>• on</li> <li>• off</li> <li>• faulty</li> </ul>
Consumption Power(watts)	Displays the power (in watts) being used by the switch.
UsageThreshold%	Lets you set a percentage of the total PoE power usage at which the switch sends a warning trap message. If the PoE power usage exceeds the threshold and SNMP traps are appropriately configured, the switch sends the <b>pethMainPowerUsageOnNotification</b> trap. If the power consumption exceeds and then falls below the threshold, the switch sends the <b>pethMainPowerUsageOffNotification</b> trap.
PowerDevice DetectType	Lets you set the power detection type that the switch uses to detect a request for power from a device connected to all ports on the switch: <ul style="list-style-type: none"> <li>• 802.3at</li> <li>• 802.3atAndLegacySupport</li> </ul> <p><b>* Note:</b></p> <p>The default setting is 802.3at. Ensure that this setting matches the setting for the detection type used by the powered devices on this switch. The 802.3at and 802.3atAndLegacySupport options are available only on PWR+ units.</p>

## Managing Power over Ethernet (PoE) using EDM

Use the information in this section to display and manage Power over Ethernet (PoE) for a standalone switch or switches in a stack.

## View PoE for Multiple Switch Units using EDM


Use this procedure to display the PoE configuration for one or more switches in a stack.

### Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **PoE**.
3. In the work area, click the **Globals - PoE Units** tab.

### Field Descriptions

Use the data in the following table to help you understand the global PoE display.

Name	Description
Power(watts)	Indicates the total power (in watts) available to the switch.
OperStatus	Indicates the power state of the switch: <ul style="list-style-type: none"> <li>• on</li> <li>• off</li> <li>• faulty</li> </ul> This is a read-only cell.
Consumption Power(watts)	Indicates the power (in watts) being used by the switch. This is a read-only cell.
UsageThreshold%	Indicates the percentage of the total power usage of the preceding switch, to which the system sends a trap. <p> <b>Important:</b></p> You must enable the traps (NotificationControlEnable) to receive a power usage trap.
PowerDevice DetectType	Indicates the power detection type that the switch uses to detect a request for power from a device connected to all ports on the switch. Values include: <ul style="list-style-type: none"> <li>• 802.3at</li> <li>• 802.3atAndLegacySupport</li> </ul>

## Configure PoE for Multiple Switch Units using EDM

Use this procedure to configure PoE for one or more switches in a stack.



### Procedure steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, click **PoE**.
3. In the work area, click the **PoE Units** tab.
4. To select a switch to edit, click the Unit.
5. In the Unit row, double-click the cell in the **UsageThreshold%** column.

6. Type a value.
7. In the Unit row, double-click the cell in the **PowerDeviceDetectType** column.
8. Select a value from the list.
9. To manage PoE for additional switch units in a stack, repeat steps 4 through 8.
10. Click **Apply** .

## Field Descriptions

Use the data in the following table to configure PoE for one or more switches in a stack.

Name	Description
Power(watts)	Indicates the total power (in watts) available to the switch. This is a read-only cell.
OperStatus	Indicates the power state of the switch: <ul style="list-style-type: none"> <li>• on</li> <li>• off</li> <li>• faulty</li> </ul> This is a read-only cell.
Consumption Power(watts)	Indicates the power (in watts) being used by the switch. This is a read-only cell.
UsageThreshold%	Specifies the percentage of the total power usage of the preceding switch, to which the system sends a trap. <p> <b>Important:</b></p> You must enable the traps (NotificationControlEnable) to receive a power usage trap.
PowerDevice DetectType	Specifies the power detection type that the switch uses to detect a request for power from a device connected to all ports on the switch. Values include: <ul style="list-style-type: none"> <li>• 802.3at</li> <li>• 802.3atAndLegacySupport</li> </ul> <p> <b>Important:</b></p> The default setting is 802.3at. Ensure that this setting matches the setting for the detection type used by the powered devices on this switch. The 802.3at and 802.3atAndLegacySupport options are available only on PWR+ units.

## Configuring PoE for Switch Ports using EDM

Use the information in this section to display and modify PoE configuration for switch ports.

 **Important:**

The procedures in this section apply only to a switch with PoE ports.

## View PoE Information for Specific Switch Ports using EDM


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

### Procedure steps

1. From the Device Physical View, select one or more ports.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. Double-click **Ports**.
5. In the work area, click the **PoE** tab.

### Field Descriptions

Use the data in the following table to display the PoE configuration for specific switch ports.

Name	Description
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Lets you enable or disable PoE on this port. By default, PoE is enabled.
PowerPairs	Displays the status of the RJ-45 pin pairs that the switch uses to send power to the ports on the switch.
DetectionStatus	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>• deliveringPower—detection found 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>Important:</b> Extreme Networks recommends that you do not use the test operational status.</p>
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Lets you set the power priority for the specified port to: <ul style="list-style-type: none"> <li>• critical</li> <li>• high</li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>low</li> </ul>
PowerLimit(watts)	<p>Specifies the maximum power that the switch can supply to a port.</p> <p>The maximum power and system default power is 32W per port for the 802.3at-compliant PoE+ model and 60W for the uPoE model.</p>
PowerUpMode	<p>Specifies the power up mode for the port. By default, the power up mode is 802dot3at.</p> <p>Following are the options:</p> <ul style="list-style-type: none"> <li>802.3af—indicates an inrush current of 400 mA to 450 mA.</li> <li>highInrush—indicates an inrush current as described by the lcut/lлим (default is 700 mA to 1.0 A).</li> <li>pre802dot3at—indicates an inrush current of 400 mA to 450 mA, which is switched to higher lлим (700 mA to 1.0 A) within 75 milliseconds, after the port is powered up.</li> <li>802dot3at—indicates an inrush current as described by the lcut/lлим (default is 700 mA to 1.0 A).</li> </ul> <p>Where, lлим represents the highest consumption level possible and lcut represents a level beyond which power consumption is regarded as an overload.</p>
Voltage(volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

## Configure PoE for Specific Switch Unit Ports using EDM

Use this procedure to modify the PoE configuration for a one or more ports on a specific switch unit.


### Procedure steps

1. From the Device Physical View, select one or more ports on a switch unit.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Chassis**.
4. Double-click **Ports**.
5. In the work area, click the **PoE** tab.
6. In the unit port row, double-click the cell in the **AdminEnable** column.
7. In the unit port row, double-click the cell in the **PowerUpMode** column.
8. Select a value from the list.
9. In the unit port row, double-click the cell in the **PowerPriority** column.
10. Select a value from the list.
11. In the unit port row, double-click the cell in the **PowerLimit(watts)** column.
12. Type a value.
13. To configure PoE for other selected ports, repeat steps **6** through **12**.

14. Click **Apply** .

## Field Descriptions

Use the data in the following table to modify PoE for a one or more specific ports.

Name	Description
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Lets you enable or disable PoE on this port. By default, PoE is enabled.
PowerUpMode	Specifies the power up mode for the port. By default, the power up mode is 802dot3af. Following are the options: <ul style="list-style-type: none"> <li>• 802.3af—indicates an inrush current of 400 mA to 450 mA.</li> <li>• highInrush—indicates an inrush current as described by the lcut/lLim (default is 700 mA to 1.0 A).</li> <li>• pre802dot3af—indicates an inrush current of 400 mA to 450 mA, which is switched to higher lLim (700 mA to 1.0 A) within 75 milliseconds, after the port is powered up.</li> <li>• 802dot3at—indicates an inrush current as described by the lcut/lLim (default is 700 mA to 1.0 A).</li> </ul> lLim represents the highest consumption level possible and lcut represents a level beyond which power consumption is regarded as an overload.
DetectionStatus	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>• deliveringPower—detection found 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>  <b>Important:</b> Extreme Networks recommends that you do not use the test operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Lets you set the power priority for the specified port to: <ul style="list-style-type: none"> <li>• critical</li> <li>• high</li> </ul>

*Table continues...*

Name	Description
	• low
PowerLimit(watts)	Specifies the maximum power that the switch can supply to a port. The maximum power and system default power is 32W per port for the 802.3at-compliant PoE+ model and 60W for the uPoE model.
Voltage(volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

## Configure PoE for Switch or Stack Ports using EDM

Use this procedure to modify the PoE configuration for a one or more switch or stack ports.

### Procedure Steps

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **PoE**.
3. In the work area, click the **PoE Ports** tab.
4. To select a switch port to edit, click the unit row.
5. In the unit port row, double-click the cell in the **AdminEnable** column.
6. Select a value from the list—**true** to enable PoE for the port, or **false** to disable PoE for the port.
7. In the unit port row, double-click the cell in the **PowerPriority** column.
8. Select a value from the list.
9. In the unit port row, double-click the cell in the **PowerLimit(watts)** column.
10. Type a value.
11. In the unit port row, double-click the cell in the **PowerUpMode**.
12. Select a value from the list.
13. To configure PoE for additional ports, repeat steps **4** through **10**.
14. Click **Apply**.


### Field Descriptions

Use the data in the following table to configure PoE for a one or more switch or stack ports.

Name	Description
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Lets you enable or disable PoE on this port. By default, PoE is enabled.

*Table continues...*



Name	Description
DetectionStatus	<p>Displays the operational status of the power-device detecting mode on the specified port:</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 on this port</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> <li>• test—detecting device in test mode</li> <li>• otherFault</li> </ul> <p> <b>Important:</b> Extreme Networks recommends that you do not use the test operational status.</p>
PowerClassifications	<p>Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.</p>
PowerPriority	<p>Lets you set the power priority for the specified port to:</p> <ul style="list-style-type: none"> <li>• critical</li> <li>• high</li> <li>• low</li> </ul>
PowerLimit(watts)	<p>Specifies the maximum power that the switch can supply to a port.</p> <p>The maximum power and system default power is 32W per port for the 802.3at-compliant PoE+ model and 60W for the uPoE model.</p>
PowerUpMode	<p>Specifies the power up mode for the port. By default, the power up mode is 802dot3at.</p> <p>Following are the options:</p> <ul style="list-style-type: none"> <li>• 802.3af—indicates an inrush current of 400 mA to 450 mA.</li> <li>• highInrush—indicates an inrush current as described by the lcut/lлим (default is 700 mA to 1.0 A).</li> <li>• pre802dot3at—indicates an inrush current of 400 mA to 450 mA, which is switched to higher lлим (700 mA to 1.0 A) within 75 milliseconds, after the port is powered up.</li> <li>• 802dot3at—indicates an inrush current as described by the lcut/lлим (default is 700 mA to 1.0 A).</li> </ul> <p>Where, lлим represents the highest consumption level possible and lcut represents a level beyond which power consumption is regarded as an overload.</p>

*Table continues...*

Name	Description
Voltage(volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

## Configuring the PoE Conservation Level Request TLV using the EDM

Use this procedure to request a specific power conservation level for an IP phone connected to a switch port.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Local Port** tab.
6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **PoeConsLevelRequest** column.
8. Type a value in the box.
9. On the toolbar, click **Apply**.

### Field Descriptions

Name	Description
PoeConsLevelRequest	Specifies the power conservation level to request for a vendor specific PD. Values range from 0 to 255. With the default value of 0, the switch does not request a power conservation level for an IP phone connected to the port.

## Configure the 802.1Q Framing TLV using EDM

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an IP phone.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Local Port** tab.

6. To select a port, click the **PortNum**.
7. In the port row, double-click the cell in the **Dot1QFramingRequest** column.
8. Select a value from the list.
9. On the toolbar, click **Apply**.

### Field Descriptions

Name	Description
Dot1QFramingRequest	<p>Specifies the frame tagging mode. Values include:</p> <ul style="list-style-type: none"> <li>• tagged—frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV.</li> <li>• non-tagged—frames are not tagged with 802.1Q priority.</li> <li>• auto—an attempt is made to tag frames based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged.</li> </ul> <p>The default tagging mode is auto.</p>

## View the PoE Conservation Level Request and 802.1Q Framing TLV Configuration using EDM

Use this procedure to display the configuration status of the PoE conservation level request and 802.1Q framing TLVs that the switch can transmit to IP phones.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Local Port** tab.

### Field Descriptions

Name	Description
Dot1QFramingRequest	<p>Displays the frame tagging mode. Values include:</p> <ul style="list-style-type: none"> <li>• tagged—frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV.</li> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• non-tagged—frames are not tagged with 802.1Q priority.</li> <li>• auto—an attempt is made to tag frames based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged.</li> </ul> <p>The default tagging mode is auto.</p>
PoeConsLevelRequest	<p>Specifies the power conservation level to request for a vendor specific PD. Values range from 0 to 255. With the default value of 0, the switch does not request a power conservation level for an IP phone connected to the port.</p>

## View PoE Conservation Level Support TLV Information using EDM

Use this procedure to display PoE conservation level information received on switch ports from an IP phone.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Vendor Specific**.
5. In the work area, click the **Neighbor PoE** tab.

### Field Descriptions

Name	Description
TimeMark	Displays the time the latest TLV-based information is received from an IP phone.
LocalPortNum	Displays the number of the switch port on which the TLV-based information is received.
Index	Displays a unique identifier for the connected IP phone.
PoeConsLevelValue	Displays the PoE conservation level supported by the IP phone connected to the switch port.

# Chapter 6: Link Layer Discovery Protocol (802.1ab)

This chapter describes the Link Layer Discovery Protocol (LLDP) (IEEE 802.1ab).

---

## Link Layer Discovery Protocol Fundamentals

This section provides conceptual information related to the configuration and management of Link Layer Discovery Protocol (LLDP).

---

## Link Layer Discovery Protocol (IEEE 802.1AB) Overview

The switch software supports the Link Layer Discovery Protocol (LLDP) (IEEE 802.1AB), which enables stations connected to a LAN to advertise their capabilities to each other, enabling the discovery of physical topology information for network management. LLDP-compatible stations can consist of any interconnection device including computers, 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.

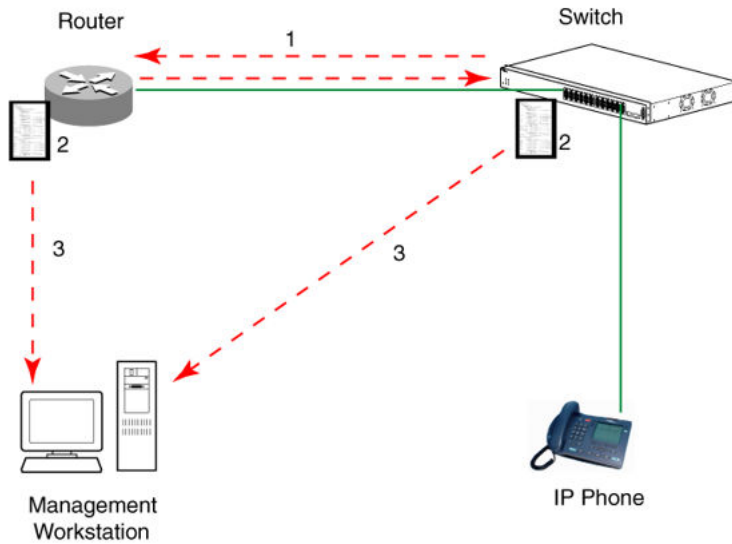
Each LLDP station:

- Advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with the switch).
- Receives network management information from adjacent stations on the same LAN.

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

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

[Figure 14: How LLDP works](#) on page 366 shows an example of how LLDP works in a network.



**Figure 14: How LLDP works**

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

## LLDP operational modes

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

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

---

## Connectivity and Management Information

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

Each LLDPDU includes the following four mandatory TLVs:

- Chassis ID TLV

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

**\* Note:**

Starting with Release 7.4.1, the Port ID TLV value changes from subtype 3 (port mac address) into subtype 5 interfaceName (<slot>/<port>).

The chassis ID value is concatenated to form a logical MSAP identifier that the recipient uses to identify the sending LLDP agent.

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 the TTL field of the 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, switch software supports the TLV extension set consisting of Management TLVs and organizational-specific TLVs. Organizational-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.

## Basic management TLV set

The basic management TLV set contains the following TLVs:

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

The switch supports IPv4 and IPv6 in band management addresses TLV and the transmission of all TLVs from the basic management TLV set is enabled by default.

The switch does not support out of band management addresses in local management address TLV. If the switch does not have active in band IPv4 or IPv6 addresses then the switch sends the MAC address in management address TLV.

## IEEE 802.1 organizational-specific TLVs

The optional IEEE 802.1 organizational-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 switch:
  - 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 organizational-specific TLVs

The optional IEEE 802.3 organizational-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 either require or can provide power over twisted-pair copper links.
- Link Aggregation TLV—Indicates the current link aggregation status of IEEE 802.3 MACs.
- Maximum Frame Size TLV—Indicates the maximum supported 802.3 frame size.

## Organizational-specific TLVs for MED devices

The optional organizational-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—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—Important in managed VoIP networks. Administrative tasks in these networks are made easier by access to inventory information about VoIP entities. The LLDP Inventory TLVs consist of the following:
  - LLDP-MED Hardware Revision TLV allows the device to advertise its hardware revision.
  - LLDP-MED Firmware Revision TLV allows the device to advertise its firmware revision.
  - LLDP-MED Software Revision TLV allows the device to advertise its software revision.
  - LLDP-MED Serial Number TLV allows the device to advertise its serial number.
  - LLDP-MED Manufacturer Name TLV allows the device to advertise the name of its manufacturer.
  - LLDP-MED Model Name TLV allows the device to advertise its model name
  - LLDP-MED Asset ID TLV allows the device to advertise its asset ID

## 802.1AB MED network policies

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

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

## Transmitting LLDPDUs

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

LLDPDU are regularly transmitted at a user-configurable transmit interval (*tx-interval*) or when any of the variables in the 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.

Beginning in Release 5.7, the transmission and reception of LLDPDUs on all Device Under Testing (DUT) ports are enabled by default.

### TLV system MIBs

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

### LLDPDU and TLV error handling

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

## 802.1AB Integration

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

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

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

### PoE conservation level request TLV

With the PoE conservation level request TLV, you can configure the switch to request that an IP Phone, connected to a switch port, operate at a specific power conservation level. The requested conservation level value for the switch can range from 0 to 255, but an IP Phone can support only maximum 243 levels. If you request a power conservation level higher than the maximum conservation level an IP Phone can support, the phone reverts to its maximum supported power conservation level. If you select a value of 0 for the PoE conservation level request, the switch does not request a power conservation level for an IP Phone.

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

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

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

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

### PoE conservation level support TLV

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

### Call server TLV

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

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

The call server TLV supports IPv4 addresses only.

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

## File server TLV

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

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

The file server TLV supports IPv4 addresses only.

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

### \* Note:

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

## 802.1Q framing TLV

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

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

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

## Phone IP TLV

IP Phones use the phone IP TLV to advertise IP Phone IP address configuration information to the switch.

The phone IP TLV supports IPv4 addresses only.

## Power via MDI TLV

The Power via MDI TLV allows network management to advertise and discover the MDI power support capabilities. Beginning in Release 5.7, this TLV also performs Data Link Layer classification using PoE-specific LLDP specified in the Clause 79 of IEEE 802.3 with additional protocol rules defined in Clause 33 (IEEE 802.3at). Clause 33 defines two power entities, Powered Device (PD) and Power Sourcing Equipment (PSE). These entities allow devices to draw or supply power over the sample generic cabling as used for data transmission.

The following fields are added to provide Data Link Layer classification capabilities:

- Power type/source/priority—Contains the power type, power source, and priority bit-map. The power type is set according to the device generating the LLDPDU. The power source describes the different definitions for PD and PSE. Power priority indicates the configured PoE priority. When the power type is PD, this field is set to the power priority configured for the device. If a PD is unable to determine its power priority or it is not configured, then this field is set to 00.
- PD Requested Power—Contains the PD requested power value. The PD requested power value is the maximum input average power which the PD wants to draw and as measured at the input to the PD.

- PSE Allocated Power—Contains the PSE allocated power value. The PSE allocated power value is the maximum input average power which the PSE expects the PD to draw at the input to the PD.

## Use Fabric Attach LLDP Extensions

The Fabric Attach (FA) agent advertises its capabilities through LLDP packets. New organizational-specific TLVs are used to export FA element data to directly-connected network components. The new TLVs use TLV type 127 as described in the 802.1ab (LLDP) standard.

### FA Element TLV

With the FA Element TLV, FA elements advertise their FA capabilities. This data forms the basis for FA element discovery and determines the state machine used by FA entities. This information is received, processed, and stored by the receiving device so that it is immediately accessible for internal applications.

FA Element TLV data integrity and source validation is supported through the use of the HMAC-SHA256 message authentication algorithm.

The Organizationally Specific FA Element TLV contains the following data:

- FA Element Type — indicates element capabilities
- FA Element Management VLAN — identifies the management VLAN
- FA Element State Data — supports the exchange of element state information
- FA Element System ID — unique system identifier used to support element discovery and tracking.

The FA Element TLV is included in all LLDPDUs when the FA service is enabled and when the per-port transmission flags associated with this TLV are enabled. FA port settings can only be viewed and not modified through the LLDP CLI interface. FA port settings must be updated using the FA CLI support.

With the FA service enabled, LLDPDUs containing proprietary TLVs are transmitted on links that may or may not have components at the far end. Since the LLDP standard dictates that unrecognized but well-formed TLVs in received LLDPDUs should be ignored, this should not cause any issues.

#### **Note:**

This behavior is different from the way other proprietary LLDP TLVs are handled. The other proprietary TLVs are only included in LLDPDUs generated on links that have recognized elements, specifically telephony gear, at the far end.

### FA I-SID/VLAN Assignment TLV

With the FA I-SID/VLAN Assignment TLV, an FA Proxy or FA Client distributes I-SID/VLAN assignments that it would like installed by an FA Server. This information is received, processed, and stored by the receiving device so that it is immediately accessible for internal applications. An FA Server uses FA I-SID/VLAN Assignment TLV to provide feedback about the requested bindings to the originating FA device.

I-SID/VLAN Assignment TLV data integrity and source validation is supported through the use of the HMAC-SHA256 message authentication algorithm.

I-SID/VLAN assignment requests can be accepted (activated) or rejected by an FA Server.

The FA I-SID/VLAN Assignment TLV is only included in a LLDPDU when complementary FA element devices (FA Proxy, FA Server or FA Client) are directly connected. The associated per-port transmit flags must be enabled as well.

The Organizationally Specific FA I-SID/VLAN Assignment TLV contains the following data:

- VLAN ID — Identifies the VLAN component of the I-SID/VLAN mapping.
- I-SID — Identifies the I-SID component of the I-SID/VLAN mapping.
- Status — Contains information related to the processing of the I-SID/VLAN mapping.

Multiple I-SID/VLAN assignments can be included in a single TLV.

All I-SID/VLAN assignments defined on an FA Proxy, as well as those received from FA Clients when external client proxy operation is enabled, start in the *pending* state. This state is updated based on feedback received from the FA Server. If an assignment is accepted by the FA Server, its state is updated to *active*. A server can also reject proposed I-SID/VLAN assignments. In this case, the assignment state is updated to *rejected*.

### TLV Transmit Flags

With the transmit flags you can choose on a per-port basis which LLDP TLVs (including the TLVs, such as Call Server TLV or FA TLVs) to include in transmitted LLDPDUs, and which to exclude. These flags are independent of the configured TLV data. Therefore, even if data for a specific TLV is configured, the TLV is only included in LLDPDUs on ports for which the TLV is enabled for transmission.

By default, the transmit flags are set to *enabled* for non-FA TLVs (the PoE Conservation Levels TLV default depends on the device's PoE support) on all ports. The transmit flags for the FA Element and FA I-SID/VLAN Assignment TLVs default to *enabled* on a FA Proxy and *disabled* on an FA Server, on all ports. The transmit flag values for the FA TLVs can only be manipulated through the FA support (with the `fa port-enable` CLI command).

---

## Configuring LLDP using CLI

The following sections provide procedures to enable and configure Link Layer Discovery Protocol (LLDP) using the CLI.

---

### Set LLDP Transmission Parameters

#### About this task

Use this procedure to set the LLDP transmission parameters.

#### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

- At the command prompt, enter the following command:

```
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>] [vendor-specific {call-server | file-
server}]
```

- Press Enter.

## Variable definitions

The following table describes the variables for the `lldp` command.

Variables	Description
<code>tx-interval &lt;5-32768&gt;</code>	Sets the interval between successive transmission cycles.
<code>tx-hold-multiplier &lt;2-10&gt;</code>	Sets the multiplier for the tx-interval used to compute the Time To Live value for the TTL TLV.
<code>reinit-delay &lt;1-10&gt;</code>	Sets the delay for the reinitialization attempt if the adminStatus is disabled.
<code>tx-delay &lt;1-8192&gt;</code>	Sets the minimum delay between successive LLDP frame transmissions.
<code>med-fast-start &lt;1-10&gt;</code>	Sets value for med-fast-start.
<code>notification-interval &lt;5-3600&gt;</code>	Sets the interval between successive transmissions of LLDP notifications.
<code>vendor-specific {call-server   file-server}</code>	Sets the vendor specific details for advertising the call server or file server details to the IP phones.

## Set LLDP Port Parameters

### About this task

Use this procedure to set the LLDP port parameters.

### Procedure

- Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

- At the command prompt, enter the following command:

```
lldp port <portlist> [status {rxOnly | txAndRx | txOnly}] [config
notification]
```

- Press Enter.

## Variable definitions

The following table describes the variables for the `lldp port` command.

Variables	Description
port <portlist>	Specifies the ports affected by the command.
status {rxOnly   txAndRx   txOnly}	<p>Sets the LLDPDU transmit and receive status on the ports.</p> <ul style="list-style-type: none"> <li>• rxonly: enables LLDPDU receive only</li> <li>• txAndRx: enables LLDPDU transmit and receive</li> </ul> <p>For LLDP support for PoE+, transmission and reception must be enabled.</p> <ul style="list-style-type: none"> <li>• txOnly: enables LLDPDU transmit only</li> </ul>
config notification	Enables notification when new neighbor information is stored or when existing information is removed. The default value is <i>enabled</i> .

## Set LLDP Media Endpoint Devices (MED)

### About this task

Use this procedure to configure LLDP Media Endpoint Devices (MED) policies for switch ports.

#### \* Note:

As a safeguard, a LLDP-MED Network Policy TLV is not sent in the LLDPDUs if the policy has the vlan-id set to value 0 (priority tagged frames).

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp med-network-policies [port <portList>] {voice|voice-signaling}
[dscp <0-63>] [priority <0-7>] [tagging {tagged|untagged}] [vlan-id
<0-4094>]
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `lldp med-network-policies` command.

Variable	Description
port <portlist>	Specifies the port or ports on which to configure LLDP MED policies.
voice	Specifies voice network policy. The default value is 46.
voice-signaling	Specifies voice signalling network policy.
dscp <0-63>	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63. The default value is 46.
priority <0-7>	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. Values range from 0–7. The default value is 6.
tagging {tagged   untagged}	Specifies the type of VLAN tagging to apply on the selected switch port or ports. <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> If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.
vlan-id <0-4094>	Specifies the VLAN identifier for the selected port or ports. Values range from 0–4094 (0 is for priority tagged frames). If you select priority tagged frames, the system recognizes only the 802.1p priority level and uses a value of 0 for the VLAN ID of the ingress port.

---

## Set the Optional Management TLVs

### About this task

Use this procedure to set the optional Management TLVs to be included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp tx-tlv [port <portlist>] [local-mgmt-addr] [port-desc] [sys-
cap] [sys-desc] [sys-name]
```

3. Press Enter.



## Variable definitions

The following table describes the variables for the `lldp tx-tlv` command.

Variables	Description
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.
port-desc	The port description TLV. This TLV is enabled by default. This TLV is enabled by default.
port <portlist>	Specifies a port or list of ports.
sys-cap	The system capabilities TLV.
sys-desc	The system description TLV. This TLV is enabled by default.
sys-name	The system name TLV. This TLV is enabled by default.
med	The Media Endpoint Device (MED) for a specific TLV.

## Set the Optional IEEE 802.1 Organizationally-Specific TLVs

### About this task

Use this procedure to set the optional IEEE 802.1 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp tx-tlv [port <portlist>] dot1 [port-protocol-vlan-id
<vlanlist>] [port-vlan-id ] [protocol-identity < [EAP] [LLDP]
[STP]>] [vlan-name <vlanlist>]
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `lldp tx-tlv dot1` command.

Variables	Description
port <portlist>	The ports affected by the command.
port-protocol-vlan-id <vlanlist>	The port and protocol VLAN ID TLV.
port-vlan-id	The port VLAN ID TLV.

*Table continues...*

Variables	Description
protocol-identity <[EAP] [LLDP] [STP]>	Protocol Identity TLV
vlan-name <vlanlist>	The VLAN name TLV.

## Set the Optional IEEE 802.3 Organizationally-Specific TLVs

### About this task

Use this procedure to set the optional IEEE 802.3 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp tx-tlv [port <portlist>] dot3 [link-aggregation][mac-phy-
config-status] [maximum-frame-size][mdi-power-support]
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `lldp tx-tlv dot3` command.

Variables	Description
port <portlist>	The ports affected by the command.
link-aggregation	The link aggregation TLV.
mac-phy-config-status	The MAC/Phy configuration or status TLV.
maximum-frame-size	Maximum Frame Size TLV.
mdi-power-support	Power via MDI TLV is sent only on ports where transmission is enabled. The power via MDI TLV, transmission of this TLV is enabled by default on all POE ports. The transmission can be enabled only on PoE ports.

## Set the Optional Organizationally Specific TLVs

### About this task

Use this procedure to set the optional organizationally specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

## Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
lldp tx-tlv [port <portlist>] med [extendedPSE] [inventory]
[location] [med-capabilities] [network-policy]
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `lldp tx-tlv med` command.

Variables	Description
port <portlist>	specifies the ports affected by the command
med-capabilities	MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted). This TLV is enabled by default.
extendedPSE	Extended PSE TLV, the transmission of this TLV is enabled by default only on POE port switches.
inventory	Inventory TLVs This TLV is enabled by default.
location	Location Identification TLV This TLV is enabled by default.
network-policy	Network Policy TLV This TLV is enabled by default.

## Set the LLDP Transmission Parameters to Default Values

### About this task

Use this procedure to set the LLDP transmission parameters to their default values.

#### \* Note:

If no parameters are specified, the default `lldp` sets all parameters to their default parameters.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
default lldp [tx-interval ] [tx-hold-multiplier ] [reinit-delay]
[tx-delay] [notification-interval] [med-fast-start]
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `default lldp` command.

Variables	Description
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 re-initialize 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 to the default value.

---

## Set the Port Parameters to Default Values

### About this task

Use this procedure to set the port parameters to their default values.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
default lldp port <portlist> [status] [config notification]
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `default lldp port` command.

Variables	Description
port <portlist>	The ports affected by the command.
status	Sets the LLDP transmit and receive status to the default value (txAndRx).
config notification	Sets the config notification to its default value (disabled).

## Set the LLDP MED Policies to Default Values

### About this task

Use this procedure to set LLDP MED policies for switch ports to default values.

**\* Note:**

If no parameter is used, both voice and voice-signaling lldp network policies are restored to default. Starting with release 5.5, a default network policy for voice id is defined on all switch ports. This have Layer 2 priority 6, DSCP 46, tagging parameter set to untagged and vlan ID 0.

**\* Note:**

As a safeguard, a LLDP-MED Network Policy TLV is not sent in the LLDPDUs, if the policy has the vlan-id set to value 0 (priority tagged frames).

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
default lldp med-network-policies {voice|voice-signaling} [port
<portList>]
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `default lldp med-network-policies` command.

Variable	Description
port <portlist>	Specifies the port or ports on which to configure default LLDP MED policies.
voice	Specifies the default voice network policy. The default value is 46.
voice-signaling	Specifies the default voice signalling network policy.

## Set the LLDP Management TLVs to default values

### About this task

Use this procedure to set the LLDP Management TLVs to their default values.

**Procedure**

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
default lldp tx-tlv port <portlist> local-mgmt-addr port-desc sys-
cap sys-desc sys-name
```

3. Press Enter.

**Variable definitions**

The following table describes the variables for the `default lldp tx-tlv` command.

Variables	Description
port <portlist>	The ports affected by the command.
port-desc	The port description TLV. This TLV is enabled by default.
sys-name	The system name TLV. This TLV is enabled by default.
sys-desc	The system description TLV. This TLV is enabled by default.
sys-cap	The system capabilities TLV. This TLV is enabled by default.
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.

**Set the Optional IEEE 802.1 and Organize Specific TLVs to Default Values****About this task**

Use this procedure to set the optional IEEE 802.1 organizationally specific TLVs to their default values.

**Procedure**

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
default lldp tx-tlv port <portlist> dot1 [port-protocol-vlan-id]
[port-vlan-id] [protocol-identity [EAP] [LLDP] [STP]] [vlan-name]
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `default lldp tx-tlv dot1` command.

Variables	Description
port <portlist>	The ports affected by the command.
port-vlan-id	The port VLAN ID TLV (default value is false: not included).
vlan-name	The VLAN Name TLV (default value is none).
port-protocol-vlan-id	The port and protocol VLAN ID TLV (default value is none).
protocol-identity [EAP] [LLDP] [STP]	The protocol identity TLV (default value is none).

## Set the Optional IEEE 802.3 and Organize Specific TLVs to Default Values

### About this task

Use this procedure to set the optional IEEE 802.3 organizationally specific TLVs to their default values.

#### \* Note:

Transmission of MDI TLVs can be enabled only on POE switch ports.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
default lldp tx-tlv port <portlist> dot3 link-aggregation mac-phy-
config-status maximum-frame-size mdi-power-support
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `default lldp tx-tlv dot3` command.

Variables	Description
port <portlist>	The ports affected by the command.

*Table continues...*

Variables	Description
mac-phy-config-status	The MAC/Phy Configuration/Status TLV (default value is false: not included).
mdi-power-support	The power via MDI TLV. This TLV is enabled by default.
link-aggregation	The link aggregation TLV (default value is false: not included).
maximum-frame-size	The maximum frame size TLV (default value is false: not included).

## Set the Default Values for the Optional TLVs for MED Devices

### About this task

Use this procedure to set default values for the optional organizationally specific TLVs for use by MED devices to be included in the transmitted LLDPDUs.

**\* Note:**

Transmission of ExtendedPSE TLVs can be enabled only on POE switch ports.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
default lldp tx-tlv port <portlist> med extendedPSE inventory
inventory location med-capabilities network-policy
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `default lldp tx-tlv med` command.

Variables	Description
port <portlist>	specifies the ports affected by the command
med-capabilities	MED Capabilities TLV (MED TLVs are transmitted only if MED Capabilities TLVs are transmitted). This TLV is enabled by default.
extendedPSE	Extended PSE TLV This TLV is enabled by default.
inventory	Inventory TLVs This TLV is enabled by default.

*Table continues...*



Variables	Description
location	Location Identification TLV This TLV is enabled by default.
network-policy	Network Policy TLV This TLV is enabled by default.

---

## Disable LLDP Features on the Port

### About this task

Use this procedure to disable LLDP features on the port.

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
no lldp [port <portlist>] [status] [config-notification]
```
3. Press Enter.

---

## Disable LLDP MED Policies for Switch Ports

### About this task

Use this procedure to disable LLDP MED policies for switch ports.

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
no lldp med-network-policies [port <portList>] {voice|voice-
signaling}
```
3. Press Enter.

## Variable definitions

The following table describes the variables for the `no lldp med-network-policies` command.

Variable	Description
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.

## Disable the Optional Management TLVs

### About this task

Use this procedure to disable the optional Management TLVs so that these TLVs are not included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
no lldp tx-tlv port <portlist> local-mgmt-addr port-desc sys-cap
sys-desc sys-name
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `no lldp tx-tlv` command.

Variables	Description
port <portlist>	The ports affected by the command.
port-desc	The port description TLV. This TLV is enabled by default.
sys-name	The system name TLV. This TLV is enabled by default.
sys-desc	The system description TLV. This TLV is enabled by default.
sys-cap	The system capabilities TLV (default value is false: not included).
local-mgmt-addr	The local management address TLV. This TLV is enabled by default.

---

## Disable the Optional IEEE 802.1 TLVs

### About this task

Use this procedure to disable the optional IEEE 802.1 TLVs so that these TLVs are not included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
no lldp tx-tlv [port <portlist>] dot1 [port-vlan-id] [vlan-name]
[port-protocol-vlan-id] [protocol-identity [EAP] [LLDP] [STP] ]
```

3. Press Enter.

---

## Disable the Optional IEEE 802.3 TLVs

### About this task

Use this procedure to disable the optional IEEE 802.3 TLVs so that these TLVs are not included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
no lldp tx-tlv port <portlist> dot3 link-aggregation mac-phy-config-
status maximum-frame-size mdi-power-support
```

3. Press Enter.

---

## Disable the Optional LLDP MED TLVs

### About this task

Use this procedure to disable the optional LLDP MED TLVs so that these TLVs are not included in the transmitted LLDPDUs.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

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

```
no lldp tx-tlv port <portlist> med extendedPSE inventory location
med-capabilities network-policy
```

3. Press Enter.

---

## View the LLDP Parameters

### About this task

Use this procedure to display the LLDP parameters.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show lldp [local-sys-data {dot1 | dot3 | med}][med-network-policies
[voice | voice-signaling] [mgmt-sys-data][neighbor {dot1 [vlan-names
| protocol-id]} | [dot3] [detail] | med [capabilities | extended-
power | inventory | location | network-policy] vendor-specific
[call-server [fa-zero-touch] | dot1q-framing | fabric-attach | file-
server | phone-ip | poe-conservation]][neighbor-mgmt-addr] [pdu-tlv-
size][rx-stats ][stats][tx-stats ][tx-tlv [dot1 | dot3 | med |
vendor-specific] [vendor-specific {call-server | dot1q-framing |
file-server | poe-conservation-request-level}]
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `show lldp` command.

Variables	Description
local-sys-data {dot1   dot3   med}	<p>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 all med 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>
med-network-policies [voice   voice-signaling]	<p>Displays Media Endpoint Devices (MED) network policies:</p> <ul style="list-style-type: none"> <li>• voice: Displays Voice Network Policies</li> <li>• voice-signaling: Displays Voice Signaling Network Policies</li> </ul>
mgmt-sys-data	The local management system data.
neighbor { dot1 [vlan-names   protocol-id] }   [dot3] [detail]   med [capabilities   extended-power   inventory   location   network-policy] vendor-specific [call-server [fa-zero-touch]   dot1q-framing   fabric-attach   file-server   phone-ip   poe-conservation ]	<p>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>• detail: displays all TLVs</li> <li>• med: displays MED TLVs</li> <li>• capabilities: Displays Capabilities TLVs</li> <li>• extended-power: Displays extended power TLV</li> <li>• inventory: Displays Inventory TLVs</li> <li>• location: Displays Location TLV</li> <li>• network-policy: Displays Network Policy TLV</li> <li>• vendor-specific: Displays vendor-specific TLVs <ul style="list-style-type: none"> <li>- call-server: Displays neighbors call-server information</li> <li>- fa-zero-touch: Displays neighbors Fabric Attach Zero Touch information</li> <li>- dot1q-framing: Displays neighbors dot1q-framing information</li> <li>- fabric-attach: Displays neighbors Fabric Attach information</li> <li>- file-server: Display neighbors file-server information</li> <li>- phone-ip: Displays neighbors phone-ip information</li> <li>- poe-conservation: Displays neighbors poe-conservation information</li> </ul> </li> </ul>
neighbor-mgmt-addr	Display 802.1ab neighbors management addresses.
pdu-tlv-size	The different TLV sizes and the number of TLVs in an LLDPDU.

*Table continues...*

Variables	Description
port	Port list.
rx-stats	The LLDP receive statistics for the local system.
stats	The LLDP table statistics for the remote system.
tx-stats	The LLDP transmit statistics for the local system.
tx-tlv {dot1   dot3   med}	<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>
vendor-specific {call-server   dot1q-framing   file-server   poe-conservation-request-level}	<p>Displays 802.1ab vendor-specific settings:</p> <ul style="list-style-type: none"> <li>• call-server: Displays call-server addresses</li> <li>• dot1q-framing: Displays 802.1Q framing tagging-mode</li> <li>• file-server: Displays file-server addresses</li> <li>• poe-conservation-request-level: Displays PoE conservation request level</li> </ul>

### Sample output: show lldp mgmt-sys-data command

Following is the sample output for the **show lldp** command with the *mgmt-sys-data* variable.

```
Switch>show lldp mgmt-sys-data
```

```

-----
      LLDP mgmt-sys-data
-----
ManagementAddr      MgmtIfId      ManagedEntityOID
-----
IPv4 192.1.1.1      0      1.3.6.4.1.45.3.78.1
-----

```

## View the LLDP Port Parameters

### About this task

Use this procedure to display the LLDP port parameters.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 |
detail | med }][rx-stats] [tx-stats] [pdu-tlv-size] [tx-tlv {dot1 |
```

```
dot3 | med | vendor-specific}] [neighbor-mgmt-addr] [neighbor {dot1
| dot3 | detail | med}
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `show lldp port` command.

Variables	Description
local-sys-data {dot1   dot3   detail   med }	<p>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>• detail: displays all organizationally specific TLV properties</li> <li>• med: displays all med 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>
rx-stats	The LLDP receive statistics for the local port.
tx-stats	The LLDP transmit statistics for the local port.
pdu-tlv-size	The different TLV sizes and the number of TLVs in an LLDPDU.
port <portlist>   all	Specifies an individual port, a list of specific ports, or all ports on the switch.
tx-tlv {dot1   dot3   med   vendor-specific}	<p>Display 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> <li>• vendor-specific: displays vendor specific TLV information</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   dot3   detail   med }	<p>The port neighbor TLVs:</p> <ul style="list-style-type: none"> <li>• dot1: displays 802.1 TLVs:</li> <li>• dot3: displays 802.3 TLVs</li> <li>• detail: displays all TLVs.</li> <li>• med: displays MED TLVs</li> <li>• vendor-specific: displays vendor specific TLV information</li> </ul>
[neighbor-mgmt-addr]	<p>The port neighbor LLDP management address.</p> <p>The switch supports IPv4 and IPv6 management addresses.</p>

**Sample: show lldp port command output**

The following is the sample output for **show lldp port** command with the *tx-tlv* variable.

```
Switch(config)#show lldp port 1-5 tx-tlv
-----
LLDP port tlvs
-----
Port  PortDesc  SysName  SysDesc  SysCap  MgmtAddr
-----
1      true      true     true     true     true
2      true      true     true     true     true
3      true      true     true     true     true
4      true      true     true     true     true
5      true      true     true     true     true
-----
```

The following is the sample output for **show lldp port** command with the *local-sys-data dot3* variable.

```
Switch(config)#show lldp port 9 local-sys-data dot3
-----
LLDP local-sys-data chassis
-----
ChassisId:  MAC address          70:7c:69:05:57:00
SysName:
SysCap:      rB / B                (Supported/Enabled)
SysDescr:
Ethernet Routing Switch 5928MTS-uPWR      HW:R0B.1      FW:7.4.0.1b   SW:v7.4.0.053
-----
LLDP local-sys-data port
-----
Port: 9
Dot3-MAC/PHY Auto-neg: supported/enabled      OperMAUtype: 2500BaseTFD
PSE MDI power:      supported/enabled      Port class: PSE
PSE power pair:      spare/not controllable  Power class: 0
PSE: Type: Type 2 PSE      Source: Primary      Priority: Low
PSE: PD requested power: 0.0 Watts
PSE: PSE allocated power: 0.0 Watts
LinkAggr: not aggregatable/not aggregated      AggrPortID: 0
MaxFrameSize: 9216
PMD auto-neg:      100Base(TXFD), (FdxA)Pause, 1000Base(TFD)
-----
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Switch(config)#
```

The following is the sample output for **show lldp port** command with the *neighbor dot3* variable.

```
Switch(config)# show lldp port 7 neighbor dot3
-----
LLDP neighbor
-----
Port: 7      Index: 3      Time: 0 days, 03:31:38
ChassisId: Network address      IPv4 10.100.41.101
PortId:      MAC address        00:0a:e4:0c:05:ac
SysCap:      TB / TB            (Supported/Enabled)
PortDesc:    IP Phone
SysDescr:    IP Telephone 2002, Firmware:0604DAD

Dot3-MAC/PHY Auto-neg: supported/enabled      OperMAUtype: 100BaseTXFD
PSE MDI power:      not supported/disabled  Port class: PD
```



```

PSE power pair:          signal/not controllable Power class: 1
PoE+ Power type: Type 2 PD
PoE+ Power priority: High
PoE+ PD requested power: 26.2w
PoE+ PSE allocated power: 26.2w
LinkAggr: not aggregatable/not aggregated      AggrPortID: 0
                                                MaxFrameSize: 1522
-----
PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD)
-----
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 2

```

## View the LLDP MED Policy Information

### About this task

Use this procedure to display the LLDP MED policy information for switch ports.

Default med-network-policy for voice have Layer 2 priority 6, DSCP 46, tagging parameter set to untagged and vlan ID 0.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```


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

```
show lldp med-network-policies [port <portList>] {voice|voice-
signaling}
```

3. Press Enter.

## Variable Definitions

The following table describes the variables for the `show lldp med-network-policies` command.

Variable	Value
port <portlist>	Specifies the port or ports for which to display LLDP MED policy information.
voice	Displays the voice network policy for which to display information. The default value is 46.
voice-signaling	Specifies the voice signalling network policy to disable.
 <b>Note:</b>	The default DSCP value is 46 and the default priority value is 6.

## Configure the PoE Conservation Level Request TLV

### About this task

Use this procedure to request a specific power conservation level for an IP Phone connected to a switch port.

#### Important:

Only Ethernet ports on switches that support PoE can request a specific power conservation level for an IP Phone.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

2. At the command prompt, enter the following command to configure PoE conservation level TLVs for connected IP Phones:

```
lldp [port <portlist>] vendor-specific poe-conservation-request-
level <0-255>
```

3. Set PoE conservation level TLVs for connected IP Phones to the default value by using the following command:

```
default lldp port <portlist> vendor-specific poe-conservation-
request-level
```

### Variable definitions

The following table describes the variables for the `lldp` command.

Variable	Description
<0-255>	Specifies the power conservation level to request for a vendor specific PD. Values range from 0 to 255. With the default value of 0, the switch does not request a power conservation level for an IP phone connected to the port.
<portList>	Specifies a port or list of ports.

## View the Switch PoE Conservation Level Request TLV Configuration

### About this task

Display PoE conservation level request configuration for local switch ports.

### Procedure

1. Enter Privileged EXEC mode:  

```
enable
```
2. Display the PoE conservation level request configuration for one or more switch ports:  

```
show lldp [port <portlist>] vendor-specific poe-conservation-request-level
```
3. Press Enter.

### Example

```
Switch>enable
Switch#configure terminal
Switch(config-if)#vendor-specific poe-conservation-request-level
-----
LLDP vendor-specific POE Request Conservation Level
-----
Unit/      POE Request
Port      Level
-----
1          0
2          0
```

## Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## View PoE Conservation Level Support TLV Information

### About this task

Use this procedure to display PoE conservation level information received on switch ports from an IP phone. To delete all call-server ip addresses configured on DUT, use `default lldp vendor-specific call-server`.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

- At the command prompt, enter the following command to view the received PoE conservation level information for one or more switch ports:

```
show lldp [port <portlist>] neighbor vendor-specific poe-
conservation
```

- Press Enter.

## Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## Configure the Switch Call Server IP Address TLV

### About this task

Use this procedure to define the local call server IP addresses that switch ports advertise to Ip Phones. You can define IP addresses for a maximum of 8 local call servers.

### Important:

The switch does not support the advertisement of IPv6 addresses to Ip Phones.

### Procedure

- Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command to define the local call server IPv4 addresses the switch advertises to Ip Phones:

```
lldp vendor-specific call-server [<1-8>] <A.B.C.D> [[<1-8>]
<A.B.C.D>] [[<1-8>] <A.B.C.D>]
```

- Enter the following command to delete call server IPv4 addresses configured on the switch:

```
default lldp vendor-specific call-server <1-8>
```

## Variable Definitions

The following table describes the variables for the `lldp vendor-specific call-server` command.

Variable	Description
<1-8>	Specifies the call server number.  * <b>Note:</b> When you advertise the IPv4 address of call server 1 only, you do not have to enter a call server number before you enter the IP address.
<A.B.C.D>	Specifies the call server IPv4 address.

## View the Switch Call Server IP Address TLV Configuration

Use this procedure to display information about the defined local call server IP address that switch ports advertise to connected IP phones.

The switch supports a maximum of 8 local call servers.

### Procedure

1. Enter Privileged EXEC mode:  
enable
2. At the command prompt, enter the following command to display call server TLV configuration information for the local switch:  
show lldp vendor-specific call-server
3. Press Enter.

### Example

```
Switch>enable
Switch#show lldp vendor-specific call-server
-----
LLDP Vendor Specific Call Servers IP addresses
-----
Configured Call Server 1: 192.0.1.1
Configured Call Server 2: 192.0.1.2
Configured Call Server 3: 192.0.2.3
-----
```

## View IP Phone Call Server IP Address TLV Information

### About this task

Use this procedure to display call server IP address information received on switch ports from an IP phone.

### Procedure

1. Enter Privileged EXEC mode:  
enable

- At the command prompt, enter the following command to display call server TLV configuration information received on specific switch ports from connected IP phones:

```
show lldp [port <portlist>] neighbor vendor-specific call-server
```

- Press Enter.

## Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## Configure the Switch File Server IP Address TLV

### About this task

Use this procedure to define the local file server IP addresses that switch ports advertise to IP phones. You can define IP addresses for a maximum of 4 local file servers.

#### \* Note:

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

#### ! Important:

The switch does not support the advertisement of IPv6 addresses to IP phones.

### Procedure

- Enter Global Configuration mode:

```
enable
configure terminal
```

- At the command prompt, enter the following command to enable file server IPv4 address advertisement to IP phones:

```
lldp vendor-specific file-server [<1-4>] <A.B.C.D> [[<1-4>]
<A.B.C.D>] [[<1-4>] <A.B.C.D>]
```

- To delete file server IPv4 addresses configured on the switch:

```
default lldp vendor-specific file-server <1-4>
```

#### \* Note:

To delete all file-server ip addresses configured on DUT, use `default lldp vendor-specific file-server` command.

## Variable Definitions

The following table describes the variables for the `lldp vendor-specific file-server` command.

Variable	Description
<1-4>	Specifies the file server number.  * <b>Note:</b> When you advertise the IPv4 address of file server 1 only, you do not have to enter a file server number before you enter the IP address.
<A.B.C.D>	Specifies the file server IPv4 address.

## View the Switch File Server IP Address TLV Configuration

Use this procedure to display information about the defined local file server IP address that switch ports advertise to connected IP phones.

You can define IP addresses for a maximum of 4 local file servers.

### ! Important:

The switch does not support the advertisement of IPv6 addresses to IP phones.

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the command prompt, enter the following command to display file server TLV configuration information for the switch:  
`show lldp vendor-specific file-server`
3. Press Enter.

### Sample: show lldp vendor-specific file-server command output

The following figure displays sample output for the `show lldp vendor-specific file-server` command.

```
Switch>enable
Switch#show lld vendor-specific file-server
-----
                        LLDP Vendor Specific File Servers IP addresses
-----
Configured Call Server 1: 192.0.1.1
Configured Call Server 2: 192.0.1.2
Configured Call Server 3: 192.0.2.3
-----
```

## View IP Phone File Server IP Address TLV Information

### About this task

Use this procedure to display information about file server IP address received on switch ports from IP phones.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command to display file server advertisement configuration information received on specific switch ports from connected IP phones:

```
show lldp [port <portlist>] neighbor vendor-specific file-server
```

3. Press Enter.

### Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

## Configure the 802.1Q Framing TLV

### Before you begin

- Enable LLDP MED capabilities.
- Enable LLDP MED network policies.

### About this task

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an IP phone.

### Procedure

1. Enter Ethernet Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface Ethernet <port>
```

2. At the command prompt, enter the following command to configure the Layer 2 frame tagging mode:

```
lldp [port <portlist>] vendor-specific dot1q-framing [tagged | non-tagged | auto]
```



- Enter the following command to set the Layer 2 frame tagging mode to default:

```
default lldp [port <portlist>] vendor-specific dot1q-framing
```

## Variable definitions

The following table describes the variables for the `lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.
[tagged   non-tagged   auto]	<p>Specifies the frame tagging mode. Values include:</p> <ul style="list-style-type: none"> <li>tagged—frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV.</li> <li>non-tagged—frames are not tagged with 802.1Q priority.</li> <li>auto—an attempt is made to tag frames based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. If there is no LLDP-MED Network Policy information available, an attempt is made to tag frames based on server configuration. If that fails, traffic is transmitted untagged.</li> </ul> <p>The default tagging mode is auto.</p>

## View the Switch 802.1Q Framing TLV Configuration

### About this task

Display the configured Layer 2 frame tagging mode for switch ports.

### Procedure

- Enter Privileged EXEC mode:
 

```
enable
```
- Display the configured Layer 2 frame tagging mode for one or more switch ports:
 

```
show lldp [port <portlist>] vendor-specific dot1q-framing
```
- Press Enter.

### Example

```
Switch(config)#interface fastethernet 1-10
Switch(config-if)#show lldp vendor-specific dot1q-framing
-----
LLDP vendor-specific 802.1Q Framing
-----
Unit/          Framing
```

Port	Tagging Mode
1	tagged
2	auto
3	auto
4	auto
5	auto
6	auto
7	auto
8	auto
9	auto
10	auto

## Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

---

## View IP phone 802.1Q Framing TLV Information

### About this task

Use this procedure to display Layer 2 frame tagging mode information received on switch ports from connected IP phones.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command to display the received Layer 2 frame tagging mode information for one or more switch ports:

```
show lldp [port <portlist>] neighbor vendor-specific dot1q-framing
```

3. Press Enter.

## Variable definitions

The following table describes the variables for the `show lldp` command.

Variable	Description
<portlist>	Specifies a port or list of ports.

---

## Configure TLV Transmission Flags

### About this task

Use this procedure to configure the transmission of optional proprietary TLVs from switch ports to IP phones.

**\* Note:**

The switch transmits configured TLVs only on ports with the TLV transmit flag enabled.

**Procedure**

1. Enter Ethernet Interface Configuration mode:

```
enable
configure terminal
interface Ethernet <port>
```

2. To select the TLVs that the switch transmits, enter the following command:

```
lldp tx-tlv [port <portList>] vendor-specific {[call-server] [dot1q-
framing] [file-server] [poe-conservation]}
```

3. To disable the transmission of optional proprietary TLVs, enter the following command:

```
no lldp tx-tlv [port <portList>] vendor-specific {[call-server]
[dot1q-framing] [file-server] [poe-conservation] }
```

4. To restore TLVs transmission to default, enter the following command:

```
default lldp tx-tlv [port <portList>] vendor-specific {[call-server]
[dot1q-framing] [file-server] [poe-conservation]}
```

**Variable Definitions**

The following table describes the parameters for the `lldp tx-tlv` command.

Variable	Value
call-server	Sets the call server TLV transmit flag state. The default state is enabled
dot1q-framing	Sets the Layer 2 priority tagging TLV transmit flag state. The default state is enabled.
file-server	Sets the file server TLV transmit flag state. The default state is enabled.
poe-conservation	Sets the PoE conservation request TLV transmit flag state. The default state is enabled.
<portList>	Specifies a port or list of ports.

**Display TLV Transmit Flag Status****About this task**

Use this procedure to display the status of transmit flags for switch ports on which IP phone support TLVs are configured.

### Procedure

1. Enter Ethernet Interface Configuration mode:
 

```
enable
configure terminal
interface Ethernet <port>
```
2. At the command prompt, enter the following command:
 

```
show lldp [port <portlist>] tx-tlv vendor-specific
```
3. Press Enter.

### Variable definitions

Use the data in the following table to use the `show lldp` command.

Variable	Definition
<portlist>	Specifies a port or list of ports.

---

## Display IP Phone IP TLV Configuration

### About this task

Use this procedure to display IP address configuration information received on switch ports from connected IP phones.

### Procedure

1. Enter Privileged EXEC mode:
 

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

```
show lldp [port <portlist>] neighbor vendor-specific phone-ip
```
3. Press Enter.

### Variable definitions

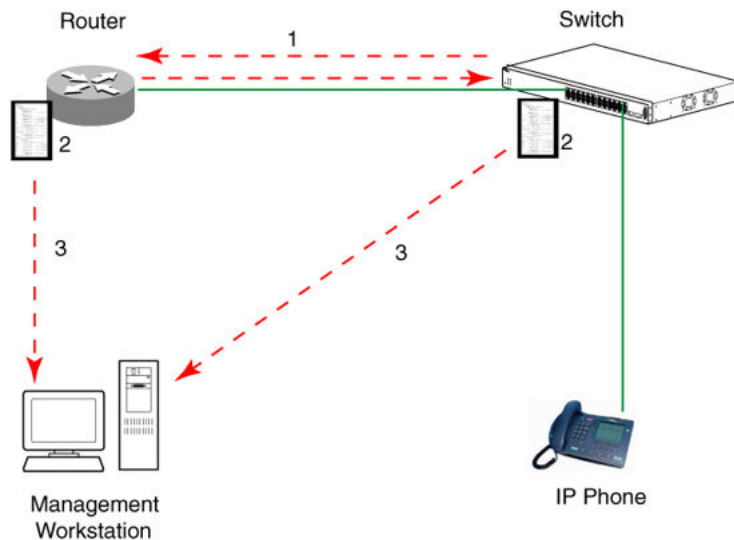
Use the data in the following table to use the `show lldp` command.

Variable	Definition
<portlist>	Specifies a port or list of ports.

## LLDP Configuration Example

By default, LLDP is enabled for Tx and Rx on all switch ports. The default value for the LLDP Tx interval is 30 seconds (LLDPDUs are sent at 30 seconds). With the default settings, only the default enabled for transmission TLVs are sent, but the switch can receive any LLDP Core, DOT1, DOT3 TLV, or Med-capabilities TLV from its peers.

The following figure shows an example of LLDP configuration. For this example, the router is connected to the switch port 1 and the IP Phone uses port 13.



**Figure 15: LLDP configuration example**

To configure the example shown in the preceding figure, you must perform the following tasks:

1. Modify the default LLDP Tx interval from (the default 30 second value) to 60 seconds.  
Note that if any modification is detected in the LLDP local-sys-data before the Tx interval expires, an LLDPDU is immediately sent on all active links to update the peers neighbor tables.
2. Enable the Port Description TLV for transmission. (contains the description of the 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 can be handled by the LLDP sending port)
15. Enable the Location Identification TLV for transmission. (indicates the physical location of the LLDP sending port; three coordinate sets are available to configure and send)
16. Enable the Extended Power-via-MDI TLV for transmission. (provides detailed informations regarding the PoE parameters of the LLDP sending device)
17. Enable the Inventory – Hardware Revision TLV for transmission. (indicates the hardware revision of the LLDP sending device)
18. Enable the Inventory – Firmware Revision TLV for transmission. (indicates the firmware revision of the LLDP sending device)
19. Enable the Inventory – Software Revision TLV for transmission. (indicates the software revision of the LLDP sending device)
20. Enable the Inventory – Serial Number TLV for transmission. (indicates the serial number of the LLDP sending device)
21. Enable the Inventory – Manufacturer Name TLV for transmission. (indicates the manufacturer name of the LLDP sending device)
22. Enable the Inventory – Model Name TLV for transmission. (indicates the model name of the LLDP sending device)
23. Configure the location information for the LLDP-MED Location Identification TLV. (There are three coordinate sets available for location advertisement.)
24. Enable the LLDP-MED Capabilities TLV for transmission (indicates the supported LLDP-MED TLVs and the LLDP-MED device type of the LLDP sending device)

## Detailed Configuration Commands

The following section describes the detailed CLI commands required to carry out the configuration depicted by [Figure 10: LLDP configuration example](#) on page 223.

### Modify the default LLDP Tx interval:

```
Switch>enable
Switch#configure terminal
Switch(config)#lldp tx-interval 60
```

### Check the new LLDP global settings:

```
Switch(config)# show lldp

802.1ab configuration:
-----
TxInterval:60
TxHoldMultiplier:4
RxInitDelay:2
TxDelay:2
NotificationInterval:5
MedFastStartRepeatCount:4
```

### Enable all LLDP Core TLVs for transmission on the router and IP Phone ports:

```
Switch(config)#interface Ethernet 1/13
Switch(config-if)#lldp tx-tlv port 1/13 port-desc
Switch(config-if)#lldp tx-tlv port 1/13 sys-name
Switch(config-if)#lldp tx-tlv port 1/13 sys-desc
Switch(config-if)#lldp tx-tlv port 1/13 sys-cap
Switch(config-if)#lldp tx-tlv port 1/13 local-mgmt-addr
```

### Check the LLDP settings of the router and IP Phone ports:

```
Switch(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
-----
```

### Enable all LLDP DOT1 TLVs for transmission on the router and IP Phone ports:

```
Switch(config-if)#lldp tx-tlv port 1/13 dot1 port-vlan-id
Switch(config-if)#lldp tx-tlv port 1/13 dot1 port-protocol-vlan-id
Switch(config-if)#lldp tx-tlv port 1/13 dot1 vlan-name
Switch(config-if)#lldp tx-tlv port 1/13 dot1 protocol-identity EAP LLDP STP
```

### Check the LLDP settings of the router and IP Phone ports:

```
Switch(config-if)# show lldp port 1/13 tx-tlv dot1
```

```
-----
LLDP port dot1 tlvs
-----
Dot1 protocols: STP,EAP,LLDP
-----
Port  PortVlanId  VlanNameList  PortProtocolVlanId  ProtocolIdentity
-----
```

```
13 true 1,3,5,7,9,117-118 1,3,5,7,9,117-118 EAP,LLDP
```

**Enable all LLDP DOT3 TLVs for transmission on the router and IP Phone ports:**

```
Switch(config-if)#lldp tx-tlv port 1/13 dot3 mac-phy-config-status
Switch(config-if)#lldp tx-tlv port 1/13 dot3 mdi-power-support
Switch(config-if)#lldp tx-tlv port 1/13 dot3 link-aggregation
Switch(config-if)#lldp tx-tlv port 1/13 dot3 maximum-frame-size
```

**Check the LLDP settings of the router and IP Phone ports:**

```
Switch(config-if)# show lldp port 1/13 tx-tlv dot3
```

```
-----
LLDP port dot3 tlvs
-----
```

Port	MacPhy ConfigStatus	MdiPower Support	Link Aggregation	MaxFrameSize
1	true	true	true	true
13	true	true	true	true

```
-----
```

**Enable all LLDP MED TLVs for transmission on the router and IP Phone ports:**

The first three commands are required to configure the location identification for the LLDP-MED Location Identification TLV.

```
Switch(config-if)#lldp location-identification civic-address country-code US city Boston
street Orlando
Switch(config-if)#lldp location-identification coordinate-base altitude 234 meters datum
WGS84
Switch(config-if)#lldp location-identification ecs-elin 1234567890
Switch(config-if)#lldp tx-tlv port 1/12-13 med med-capabilities
Switch(config-if)#lldp tx-tlv port 1/12-13 med network-policy
Switch(config-if)#lldp tx-tlv port 1/12-13 med location
Switch(config-if)#lldp tx-tlv port 1/12-13 med extendedPSE
Switch(config-if)#lldp tx-tlv port 1/12-13 med inventory
```

**Check the new LLDP settings of the router and IP Phone ports:**

```
Switch(config-if)#show lldp tx-tlv med
```

```
-----
LLDP port med tlvs
-----
```

Port	Med Capabilities	Network Policy	Location	Extended PSE	Inventory
12	true	true	true	true	true
13	true	true	true	true	true

```
-----
```

MED TLVs are transmitted only if Med-Capabilities TLV is transmitted

**Enable all the LLDP Vendor Specific TLVs for transmission on the IP Phone ports:**

```
Switch(config-if)#lldp tx-tlv port 1/13 vendor-specific call-server
Switch(config-if)#lldp tx-tlv port 1/13 vendor-specific dot1q-framing
Switch(config-if)#lldp tx-tlv port 1/13 vendor-specific file-server
Switch(config-if)#lldp tx-tlv port 1/13 vendor-specific poe-conservation
```



**Check the LLDP settings of the IP Phone port:**

```
Switch(config-if)#show lldp port 1/13 tx-tlv vendor-specific
```

LLDP port Vendor-Specific TLVs							
Unit/ Port	POE Conservation Request	Call Server	File Server	Dot1Q Framing	FA Element Type	FA I-SID/ VLAN Asgns	
13	true	true	true	true	n/a	n/a	

## Configuring LLDP using the EDM

The following sections provide procedures to enable and configure Link Layer Discovery Protocol (LLDP) using the EDM.

### LLDP configuration using EDM

Use the information in this section to configure and view LLDP global and transmit properties for local and neighbor systems.

### Configure LLDP Globally using EDM

Use the following procedure to configure LLDP transmit properties and view remote table statistics.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Globals** tab.
6. Edit global LLDP transmit properties.
7. Click **Apply** .

#### Globals Tab Field Descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
lldpMessageTxInterval	Indicates the interval, in seconds, at which LLDP frames are transmitted on behalf of this LLDP agent.

*Table continues...*

Name	Description
IldpMessageTx HoldMultiplier	Indicates the time-to-live value expressed as a multiple of the object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, is expressed by the following formula: $TTL = \min(65535, (IldpMessageTxInterval * IldpMessageTxHoldMultiplier))$ 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	Indicates the IldpReinitDelay indicates the delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins.
IldpTxDelay	Indicates 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	Controls the transmission of LLDP notifications. The agent must not generate more than one IldpRemTablesChange notification-event in the indicated period, where a <i>notification-event</i> 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.
RemTablesLast ChangeTime	Indicates the value of the sysUpTime object (defined in IETF RFC 3418) at the time an entry is created, modified, or deleted in tables associated with the IldpRemoteSystemsData objects, and all LLDP extension objects associated with remote systems. An NMS can use this object to reduce polling of the IldpRemoteSystemsData objects.
RemTablesInserts	Indicates the number of times the complete set of information advertised by a particular MSAP is inserted into tables 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

*Table continues...*

Name	Description
	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	Indicates the number of times the complete set of information advertised by a particular MSAP is deleted from tables 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	Indicates the number of times the complete set of information advertised by a particular MSAP can not be entered into tables in IldpRemoteSystemsData and IldpExtensions objects because of insufficient resources.
RemTablesAgeouts	Indicates the number of times the complete set of information advertised by a particular MSAP is deleted from tables in 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	Indicates the number of times the fast start LLDPDU is sent during the activation of the fast start mechanism defined by LLDP-MED.

## Configure Port LLDP using EDM

### About this task

Configure the optional TLVs to include in the LLDP Data Units transmitted by each port.

### Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. In the work area, click the **Port** tab.
6. To configure LLDP for a port, double-click a cell in a port row under a column heading.
7. Click **Apply**.

8. Optionally, to configure parameters for multiple ports, you can use the Make Selection section as below.
9. In the work area, in the Make Selection section of the Multiple Port Configuration pane, click the Switch/Stack/Ports ellipsis (...) to open the Port Editor dialog.
10. In the Port Editor window, click the ports you want to configure.

**\* Note:**

If you want to configure all ports, click **All**.


11. Click **OK** to return to the Make Selection pane.  
The ports you selected appear in the Switch/Stack/Ports box.
12. To change the configuration of the selected ports, in the Multiple Port Configuration pane, double-click the cell beneath the column heading that represents the parameter you want to change and do one of the following:
  - If applicable, select a value from a drop-down list.
  - Otherwise, type a value in the cell.
13. In the Make Selection pane, click **Apply Selection**.  
The changes appear in the table.
14. **(Optional)** Click **Clear Selection** to clear Multiple Port Configurations or click **Hide Non-Editable** to display only those parameters that are editable in the Multiple Port Configuration pane for the selected ports.
15. On the toolbar, click **Apply**.

**Port Tab Field Descriptions**

Use the data in the following table to use the **Port** tab.

Name	Description
PortNum	Indicates the port number. This is a read-only cell.
AdminStatus	Indicates the administratively desired status of the local LLDP agent: <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> <li>• txAndRx: the LLDP agent transmits and receives LLDP frames on this port. To enable LLDP support for PoE+, this option must be enabled. By default, this option is enabled on all the PWR+ switch ports.</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>

*Table continues...*

Name	Description
NotificationEnable	Controls, on a per-port basis, whether notifications from the agent are enabled. <ul style="list-style-type: none"> <li>• true: indicates that notifications are enabled</li> <li>• false: indicates that notifications are disabled.</li> </ul>
TLVsTxEnable	Sets the optional Management TLVs to be included in the transmitted LLDPDUs: <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><b>Note:</b></p> <p> The Local Management tab controls Management Address TLV transmission.</p>
VLANTxEnable(dot1)	Specifies whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is included in the transmitted LLDPDUs.
TLVsTxEnable(dot3)	Sets the optional IEEE 802.3 organizationally defined TLVs to be included in the transmitted LLDPDUs: <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)	Identifies which MED system capabilities are supported on the local system. This is a read-only cell.
TLVsTxEnable(med)	Sets the optional organizationally defined TLVs for MED devices to include in the transmitted LLDPDUs. <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> <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> <p>The preceding list of TLVs are enabled by default.</p>
NotifyEnable(med)	Enables or disables the topology change traps on this port.

## View LLDP TX Statistics using EDM

Use the following procedure to display LLDP transmit statistics by port.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **TX Stats** tab.

### TX Stats Tab Field Descriptions

Use the data in the following table to use the **TX Stats** tab fields.

Name	Description
PortNum	Indicates the port number
FramesTotal	Indicates the number of LLDP frames transmitted by this LLDP agent on the indicated port

### Graph LLDP Transmit Statistics using EDM

Use the following procedure to graph LLDP transmit statistics

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **TX Stats** tab.
6. In the table, select the port for which you want to display statistics.
7. On the toolbar, click **Graph**.
8. Highlight a data column to graph.
9. On the toolbar, click a graph button.

### View LLDP RX Statistics using EDM

Use the following procedure to display LLDP receive statistics by port.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **RX Stats** tab.

## RX Stats Tab Field Descriptions

Use the data in the following table to use the **RX Stats** tab.

Name	Description
PortNum	Indicates the port number.
FramesDiscardedTotal	Indicates the number of LLDP frames received on the port and discarded for any reason. This counter provides an indication that LLDP header formatting problems exist with the local LLDP agent in the sending system, or that LLDPDU validation problems exist with the local LLDP agent in the receiving system.
FramesErrors	Indicates the number of invalid LLDP frames received on the port, while the LLDP agent is enabled.
FramesTotal	Indicates the number of valid LLDP frames received on the port, while the LLDP agent is enabled.
TLVsDiscardedTotal	Indicates the number of LLDP TLVs discarded for any reason.
TLVsUnrecognizedTotal	Indicates the number of LLDP TLVs received on a given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001–111 1110) in Table 9.1 of IEEE 802.1ab-2004. An unrecognized TLV can be a basic management TLV from a later LLDP version.
AgeoutsTotal	Represents the number of age-outs that occurred on a given port. An age-out is "the number of times the complete set of information advertised by a particular MSAP is deleted from tables in 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.

## Graph LLDP RX Statistics using EDM

Use the following procedure to graph LLDP receive statistics.

### Procedure steps

1. From the navigation tree, double-click **Edit**.

2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **RX Stats** tab.
6. In the table, select the port for which you want to display statistics.
7. On the toolbar, click **Graph**.
8. Highlight a data column to graph.
9. On the toolbar, click a graph button.

## View LLDP Local System Information using EDM

Use the following procedure to display LLDP properties for the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Local System** tab.

### Local System Tab Field Descriptions

Use the data in the following table to use the **Local System** tab.

Name	Description
ChassisIdSubtype	Indicates 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	Indicates the chassis ID.
SysName	Indicates the local system name.
SysDesc	Indicates the local system description.
SysCapSupported	Indicates the system capabilities supported on the local system.

*Table continues...*



Name	Description
SysCapEnabled	Indicates the system capabilities that are enabled on the local system
DeviceClass	Indicates the MED device class.
HardwareRev	Indicates the vendor-specific hardware revision string.
FirmwareRev	Indicates the vendor-specific firmware revision string.
SoftwareRev	Indicates the vendor-specific software revision string.
SerialNum	Indicates the vendor-specific serial number.
MfgName	Indicates the vendor-specific manufacturer name.
ModelName	Indicates the vendor-specific model name.
AssetID	Indicates the vendor-specific asset tracking identifier
DeviceType	Defines the type of Power-via-MDI (PoE). <ul style="list-style-type: none"> <li>• pseDevice</li> <li>• pdDevice</li> <li>• none</li> </ul>
PDPowerSource	Defines the type of PD Power Source.
PDPowerReq	Specifies the value of the power required in 0.1 W increments by a PD.
PSEPowerSource	Defines the type of PSE Power Source (primary or back-up).
PDPowerPriority	Defines the Powered Device (PD) power priority. <ul style="list-style-type: none"> <li>• critical</li> <li>• high</li> <li>• low</li> </ul>

## View LLDP Local Port Information using EDM

Use the following procedure to display LLDP port properties for the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Local Port** tab.

### Local Port Tab Field Descriptions

Use the data in the following table to use the **Local Port** tab.

Name	Description
PortNum	Indicates the port number.
PortIdSubtype	Indicates 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> <li>• networkAddress</li> <li>• interfaceName</li> <li>• agentCircuitId</li> <li>• local.</li> </ul>
PortId	Indicates the string value used to identify the port component associated with a given port in the local system.
PortDesc	Indicates the string value used to identify the 802 LAN station port description associated with the local system. If the local agent supports IETF RFC 2863, the PortDesc object has the same value as the ifDescr object.

## View LLDP Local Management Information using EDM

Use the following procedure to display LLDP management properties for the local system.

### Procedure steps


1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostic tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Local Management** tab.

### Local Management Tab Field Descriptions

Use the data in the following table to use the **Local Management** tab.

Name	Description
AddrSubtype	Indicates the type of management address identifier encoding used in the associated Addr object.
Addr	Indicates the string value used to identify the management address component associated with the local system. This address is used to contact the management entity. The switch supports IPv4 and IPv6 management addresses.

*Table continues...*

Name	Description
	<p><b>Note:</b></p> <p> If you configure both IPv4 and IPv6 management addresses, the switch displays each on a separate row.</p>
AddrLen	Indicates the total length of the management address subtype and the management address fields in LLDPDUs transmitted by the local LLDP agent. The management address length field is needed so that the receiving systems that do not implement SNMP are not required to implement the family numbers/ address length equivalency table to decode the management address.
AddrIfSubtype	Identifies the numbering method used to define the interface number associated with the remote system. <ul style="list-style-type: none"> <li>• unknown</li> <li>• ifIndex</li> <li>• systemPortNumber</li> </ul>
AddrIfId	Indicates the integer value used to identify the interface number of the management address component associated with the local system.
AddrOID	Indicates the value used to identify the type of hardware component or protocol entity associated with the management address advertised by the local system agent.
AddrPortsTxEnable	Specifies the ports on which the local system management address TLVs are transmitted in the LLDPDUs.

### Enabling or disabling LLDP Management Address TLV transmission using EDM

Use the following procedure to enable or disable the transmission of Management Address TLVs on the local system.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Local Management** tab.
6. Double-click the cell in the **AddPortsTxEnable** column for an IPv4 or IPv6 row.
7. To enable the transmission of Management Address TLVs, select one or more port numbers.

#### OR

To disable the transmission of Management Address TLVs, deselect one or more port numbers.

8. Click **Ok**.

9. On the toolbar, click **Apply**.

## View LLDP Neighbor Information using EDM

Use the following procedure to display LLDP properties for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Neighbor** tab.

### Neighbor Tab Field Descriptions

Use the data in the following table to use **Neighbor** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry. For more information about TimeFilter, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ChassisIdSubtype	Indicates the type of encoding used to identify the remote system chassis: <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	Indicates the remote chassis ID.
SysCapSupported	Identifies the system capabilities supported on the remote system.
SysCapEnabled	Identifies the system capabilities that are enabled on the remote system.
SysName	Indicates the remote system name.

*Table continues...*

Name	Description
SysDesc	Indicates the remote system description.
PortIdSubtype	Indicates the type of encoding used to identify the remote port. <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	Indicates the remote port ID.
PortDesc	Indicates the remote port description.

## View LLDP Neighbor Management Information using EDM

Use the following procedure to display LLDP management properties for the remote system.

### Procedure steps


1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostic tree, click **802.1AB**.
4. In the 802.1AB tree, click **LLDP**.
5. In the work area, click the **Neighbor Mgmt Address** tab.

### Field Descriptions

The following table describes the fields associated with LLDP management properties for the remote system.

Name	Description
TimeMark	Indicates the TimeFilter for this entry. Value will be 0 starting with Release 7.4.1.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
AddrSubtype	Indicates the type of encoding used in the associated Addr object.

*Table continues...*

Name	Description
Addr	<p>Indicates the management address associated with the remote system. The switch supports IPv4 and IPv6 management addresses.</p> <p><b>Note:</b></p> <p> If you configure both IPv4 and IPv6 management addresses, the switch displays each on a separate row.</p>
AddrIfSubtype	<p>Indicates the numbering method used to define the interface number associated with the remote system.</p> <ul style="list-style-type: none"> <li>• unknown</li> <li>• ifIndex</li> <li>• systemPortNumber</li> </ul>
AddrIfId	<p>Indicates the integer value used to identify the interface number of the management address component associated with the remote system.</p>
AddrOID	<p>Indicates the value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.</p>

## View LLDP Unknown TLV Information using EDM

Use the following procedure to display details about unknown TLVs received on the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Unknown TLV** tab.

### Unknown TLV Tab Field Descriptions

Use the data in the following table to use **Unknown TLV** tab fields.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port which receives the remote system information.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.

*Table continues...*

Name	Description
UnknownTLVType	Indicates the value extracted from the type field of the unknown TLV.
UnknownTLVInfo	Indicates the value extracted from the value field of the unknown TLV.

## View LLDP Organizational Defined Information using EDM

Use the following procedure to display organizational-specific properties for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **LLDP**.
5. On the work area, click the **Organizational Defined Info** tab.

### Organizational Defined Info Tab Field Descriptions

Use the data in the following table to use **Organizational Defined Info** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port that receives the remote system information.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
OrgDefInfoOUI	Indicates the Organizationally Unique Identifier, as defined in IEEE 802-2001, is a 24 bit (three octets) globally unique assigned number referenced by various standards, of the information received from the remote system.
OrgDefInfoSubtype	Indicates the integer value used to identify the subtype of the organizationally defined information received from the remote system. The subtype value is required to identify different instances of organizationally defined information that cannot be retrieved without a unique identifier that indicates the particular type of information in the information string.
OrgDefInfoIndex	Represents an arbitrary local integer value used by this agent to identify a particular unrecognized organizationally defined information instance, unique only for the OrgDefInfoOUI and lldpRemOrgDefInfoSubtype of the same remote system. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot. It is

*Table continues...*

Name	Description
	unlikely that the IldpRemOrgDefInfoIndex will wrap between reboots.
OrgDefInfo	Indicates the string value used to identify the organizationally defined information of the remote system. The encoding for this object is the same as that defined for SnmpAdminString TC.

## LLDP Port dot1 configuration using EDM

Use the information in this section to configure and view IEEE 802.1 LLDP information.

### View Local VLAN ID Information using EDM

Use the following procedure to display LLDP VLAN ID properties for the local system.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Local VLAN Id** tab.

#### Local Id Tab Field Descriptions

Use the data in the following table to use **Local VLAN Id** tab.

Name	Description
PortNum	Indicates the port number.
VlanId	Indicates the local port VLAN ID. A value of zero is used if the system does not know the PVID.

### View LLDP Local Protocol VLAN Information using EDM

Use the following procedure to display LLDP local protocol VLAN properties for the local system and to enable or disable the transmission of this information from a specified port.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Local Protocol VLAN** tab.
6. To select a port to edit, click the port row.



7. In the port row, double-click the cell in the **ProtoVlanTxEnable** column.
8. Select a value from the list—**true** to enable transmitting local port and protocol VLAN information from the port, or **false** to disable transmitting local port and protocol VLAN information from the port.
9. Click **Apply** .

### Local Protocol VLAN Tab Field Descriptions

Use the data in the following table to use the **Local Protocol VLAN** tab fields.

Name	Description
PortNum	Indicates the port number.
ProtoVlanId	Indicates the ID of the port and protocol VLANs associated with the local port. A value of zero is used if the system does not know the protocol VLAN ID (PPVID).
ProtoVlanSuported	Indicates whether the local port supports port and protocol VLANs.
ProtoVlanEnabled	Indicates whether the port and protocol VLANs are enabled on the local port.
ProtoVlanTxEnable	Specifies whether the corresponding local port and protocol VLAN information are transmitted from the port.

### View LLDP Local VLAN Name Information using EDM

Use the following procedure to display LLDP VLAN Name properties for the local system and to enable or disable the transmission of this information from a specified port.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Local VLAN Name** tab.
6. To select a port to edit, click the port row.
7. In the port row, double-click the cell in the **VlanNameTxEnable** column.
8. Select a value from the list—**true** to enable transmitting local VLAN name information from the port, or **false** to disable transmitting local VLAN name information from the port.
9. Click **Apply** .

### Local VLAN Name Tab Field Descriptions

Use the data in the following table to use the **Local VLAN Name** tab.

Name	Description
PortNum	Indicates the port number.
VlanId	Indicates the integer value used to identify the IEEE 802.1Q VLAN IDs with which the given port is compatible.
VlanName	Indicates the string value used to identify the VLAN name identified by the VLAN ID associated with the given port on the local system. This object contains the value of the dot1QVLANStaticName object (defined in IETF RFC 2674) identified with the given IldpXdot1LocVlanId.
VlanNameTxEnable	Specifies whether the corresponding Local System VLAN name instance is transmitted from the port.

## View LLDP Local Protocol Information using EDM

Use the following procedure to display LLDP protocol properties for the local system and to enable or disable the transmission of this information from a specified port.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Local Protocol** tab.
6. To select a port to edit, click the port row.
7. In the port row, double-click the cell in the **VlanNameTxEnable** column.
8. Select a value from the list—**true** to enable transmitting local protocol information from the port, or **false** to disable transmitting local protocol information from the port.
9. Click **Apply** .

### Local ProtocolTab Field Descriptions

Use the data in the following table to use the **Local Protocol** tab.

Name	Description
PortNum	Indicates the port number.
ProtocolIndex	Indicates the arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	Indicates the octet string value used to identify the protocols associated with the given port of the local system.
ProtocolTxEnable	Specifies whether the corresponding Local System Protocol Identity instance is transmitted on the port.

## View LLDP Neighbor VLAN ID Information using EDM

Use the following procedure to view the LLDP VLAN ID properties for the remote system.

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Neighbor VLAN Id** tab.

## Neighbor VLAN ID Tab Field Descriptions

Use the data in the following table to use the **Neighbor VLAN ID** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
VlanId	Indicates 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.

## View LLDP Neighbor Protocol VLAN Information using EDM

Use the following procedure to display LLDP protocol VLAN properties for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Neighbor Protocol VLAN** tab.

## Neighbor Protocol VLAN Tab Field Descriptions

Use the data in the following table to use the **Neighbor Protocol VLAN** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.

*Table continues...*

Name	Description
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ProtoVlanId	Indicates the ID of the port and protocol VLANs associated with the remote port. A value of zero is used if the system does not know the protocol VLAN ID (PPVID).
ProtoVlanSuported	Indicates whether the remote port supports port and protocol VLANs.
ProtoVlanEnabled	Indicates whether the port and protocol VLANs are enabled on the remote port.

## View LLDP Neighbor VLAN Name Information using EDM

Using the following procedure to display LLDP VLAN name properties for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Neighbor VLAN Name** tab.

### Neighbor VLAN Name Tab Field Descriptions

Use the data in the following table to use the **Neighbor VLAN Name** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
VlanId	Indicates the integer value used to identify the IEEE 802.1Q VLAN IDs with which the remote port is compatible.
VlanName	Indicates the VLAN name identified by the VLAN ID associated with the remote system.

## View LLDP Neighbor Protocol Information using EDM

Use the following procedure to display LLDP protocol properties for the remote system.

## Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot1**.
5. On the work area, click the **Neighbor Protocol** tab.

## Neighbor Protocol Tab Field Descriptions

Use the data in the following table to use the **Neighbor Protocol** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
ProtocolIndex	Represents an arbitrary local integer value used by this agent to identify a particular protocol identity.
ProtocolId	Indicates the protocols associated with the remote port.

---

## LLDP Port dot3 configuration using EDM

Use the information in this section to configure and view IEEE 802.3 LLDP information.

## View LLDP Local Port Auto-Negotiation Information using EDM

Use the following procedure to display LLDP auto-negotiation properties for the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Local Port Auto-negotiation** tab.

## Local Port Auto-negotiation Tab Field Descriptions

Use the data in the following table to use the **Local Port Auto-negotiation** tab.

Name	Description
PortNum	Indicates the port number.
AutoNegSupported	Indicates whether the local port supports Auto-negotiation.
AutoNegEnabled	Indicates whether Auto-negotiation is enabled on the local port.
AutoNegAdvertisedCap	Contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the local port on the system.
OperMauType	Indicates the value that indicates the operational MAU type of the given port on the local system.

## View LLDP Local PoE Information using EDM

Use the following procedure to display LLDP PoE properties for the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Local PoE** tab.

### Local PoE Tab Field Descriptions

Use the data in the following table to use the **Local PoE** tab.

Name	Description
PortNum	Indicates the port number.
PowerPortClass	Indicates the port Class of the local port.
PowerMDISupported	Indicates whether MDI power is supported on the local port.
PowerMDIEnabled	Indicates whether MDI power is enabled on the local port.
PowerPairControlable	Indicates the value derived from the value of the pethPsePortPowerPairsControlAbility object (defined in IETF RFC 3621), this value is used to indicate whether pair selection can be controlled on the local port.
PowerPairs	Contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the local port: <ul style="list-style-type: none"> <li>• signal</li> <li>• spare</li> </ul>
PowerClass	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> </ul>

*Table continues...*

Name	Description
	<ul style="list-style-type: none"> <li>• class2</li> <li>• class3</li> <li>• class4</li> </ul>

## View Local Link Aggregate Tab using EDM

Use the following procedure to display LLDP link aggregation properties for the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Local Link Aggregate** tab.

### Local Link Aggregate Tab Field Descriptions

Use the data in the following table to use the **Local Link Aggregate** tab.

Name	Description
PortNum	Indicates the port number.
LinkAggStatus	Specifies the link aggregation capabilities and the current aggregation status of the link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation. If the port is not in a link aggregation state or does not support link aggregation, this value is set to zero.

## View LLDP Local Maximum Frame Information using EDM

Use the following procedure to display LLDP maximum frame size properties for the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Local Max Frame** tab.

### Local Max Frame Tab Field Descriptions

Use the data in the following table to use the **Local Max Frame** tab.

Name	Description
PortNum	Indicates the port number.
MaxFrameSize	Indicates the maximum frame size for the port.

## View LLDP Neighbor Port Auto-Negotiation Information using EDM

Use the following procedure to display LLDP auto-negotiation properties for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Neighbor Port Auto-negotiation** tab.

### Neighbor Port Auto-negotiation Tab Field Descriptions

Use the data in the following table to use the **Neighbor Port Auto-negotiation** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
AutoNegSupported	Indicates the truth value used to indicate whether the given port (associated with a remote system) supports Auto-negotiation.
AutoNegEnabled	Indicates whether Auto-negotiation is enabled on the remote port.
AutoNegAdvertisedCap	Contains the value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) associated with the remote port.
OperMauType	Indicates the value that indicates the operational MAU type of the given port on the remote system.

## View LLDP Neighbor PoE Information using EDM

Use the following procedure to display LLDP PoE properties for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.



4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Neighbor PoE** tab.

### Neighbor PoE Tab Field Descriptions

Use the data in the following table to use the **Neighbor PoE** tab.

Field	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PowerPortClass	Indicates the port Class of the remote port.
PowerMDISupported	Indicates whether MDI power is supported on the remote port.
PowerMDIEnabled	Indicates whether MDI power is enabled on the remote port.
PowerPairControlable	Indicates the value derived from the value of the pethPsePortPowerPairsControlAbility object (defined in IETF RFC 3621), this value is used to indicate whether pair selection can be controlled on the remote port.
PowerPairs	Contains the value of the pethPsePortPowerPairs object (defined in IETF RFC 3621) for the remote port. <ul style="list-style-type: none"> <li>• signal</li> <li>• spare</li> </ul>
PowerClass	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>

### View LLDP Neighbor Link Aggregation Information using EDM

Use the following procedure to display LLDP link aggregation properties for the remote system.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.

5. On the work area, click the **Neighbor Link Aggregate** tab.

### Neighbor Link Aggregate Tab Field Descriptions

Use the data in the following table to use the **Neighbor Link Aggregate** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
LinkAggStatus	Specifies the link aggregation capabilities and the current aggregation status of the remote link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation. If the port is not in a link aggregation state or does not support link aggregation, this value is set to zero.

### View LLDP Neighbor Maximum Frame Information using EDM

Use the following procedure to display LLDP maximum frame size properties for the remote system.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port dot3**.
5. On the work area, click the **Neighbor Max Frame** tab.

### Neighbor Max Frame Tab Field Descriptions

Use the data in the following table to use the **Neighbor Max Frame** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Indicates the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
MaxFrameSize	Indicates the maximum frame size for the remote port.

## LLDP Port MED configuration using EDM

Use the information in this section to configure and view LLDP Media Endpoint Devices (MED) information.

## LLDP MED Policy Management using EDM

Use the information in this section to view, create, and edit LLDP MED policies for the switch.

### View LLDP MED Policies using EDM

Use this procedure to view LLDP MED policy properties for the local system.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.

#### Field Description

Use the data in the following table to help you understand the LLDP MED local policy display.

Name	Description
PortNum	Indicates the port number
PolicyAppType	Shows the policy application type.
PolicyVlanID	Indicates the extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value of 0 is used if the device is using priority tagged frames, meaning that only the 802.1p priority level is significant and the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the local port. The default value is 6.
PolicyDscp	Contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the given port on the local system. The default value is 46.
PolicyTagged	Indicates whether the application is using a tagged VLAN, untagged VLAN, or does not support a port based VLAN operation.

### Create LLDP MED Policies using EDM

Use this procedure to create a new LLDP MED policy for the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.
6. Click **Insert** .
7. To select a port to create a policy for, click the **PortNum** ellipsis.
8. Click **Ok** .
9. In the **PolicyAppType** section, select one or both checkboxes.
10. To select a VLAN identifier for the selected port, click the **PolicyVlanID** ellipsis.
11. Click **Ok** .
12. Double-click the **PolicyPriority** field.
13. Type a priority value.
14. Double-click the **PolicyDscp** field.
15. Type a DSCP value.
16. To use a tagged VLAN, select the **PolicyTagged** checkbox.

**OR**

To use an untagged VLAN, clear the **PolicyTagged** checkbox.

17. Click **Insert** .

### Field Descriptions

Use the data in the following table to create a new LLDP MED policy for the local system.

Name	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 signalling 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.

*Table continues...*

Name	Description
PolicyPriority	Specifies the value of the 802.1p priority that applies to the selected switch port or ports. Values range from 0–7. The default value is 6.
PolicyDscp	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63. The default value is 46.
PolicyTagged	<p>Specifies the type of VLAN tagging to apply on the selected switch port or ports.</p> <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>

### Edit LLDP MED Policies using EDM

Use this procedure to edit a previously configured LLDP MED policy for the local system.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. To select a policy to edit, click the **PortNum**.
6. In the policy row, double-click the cell in the **PolicyVlanID** column.
7. Select a VLAN from the list.
8. Click **Ok**.
9. In the policy row, double-click the cell in the **PolicyPriority** column.
10. Edit the policy priority value.
11. In the policy row, double-click the cell in the **PolicyDscp** column.
12. Edit the policy DSCP value.
13. In the policy row, double-click the cell in the **PolicyTagged** column.
14. Select a value from the list.
15. Click **Apply**.

#### Field Descriptions

Use the data in the following table to edit a previously configured LLDP MED policy for the local system.

Name	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 signalling 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. The default value is 6.
PolicyDscp	Specifies the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the selected switch port or ports. Values range from 0–63. The default value is 46.
PolicyTagged	Specifies the type of VLAN tagging to apply on the selected switch port or ports. <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>

## Delete LLDP MED Policies using EDM

Use this procedure to delete a LLDP MED policy.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, double-click **Port MED**.
5. In the work area, click the **Local Policy** tab.
6. To select a policy to delete, click the **PortNum**.
7. Click **Delete** .

## Local Location Information Management using EDM

Use the information in this section to view and add local location information for remote network devices connected to a switch or stack.

### View Device Location Information using EDM

Use this procedure to display local location information for remote network devices connected to a switch or stack.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Local Location** tab.

#### Field Descriptions

Use the data in the following table to help you understand the remote device local location information display.

Name	Description
PortNum	Identifies the port number of the local system to which the remote device is connected.
LocationSubtype	Indicates the location subtype advertised by the remote device. <ul style="list-style-type: none"> <li>• unknown</li> <li>• coordinateBased—location information is based on geographical coordinates of the remote device</li> <li>• civicAddress—location information is based on the civic address of the remote device</li> <li>• elin—location information is based on the Emergency Location Information Number (ELIN) of the remote device</li> </ul>
LocationInfo	Displays local location information advertised by the remote device. The information displayed in this cell is directly associated with the location subtype value.

### Add ELIN based Device Location Information using the EDM

Use this procedure to add information to the local location table for remote network devices connected to a switch or stack, based on an Emergency Location Information Number (ELIN).

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.

3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Local Location** tab.
6. In the port row with **elin** as the location subtype, double-click the cell in the **LocationInfo** column.
7. Type an alphanumeric value from 10 to 25 characters in length.
8. Click **Apply** .

### Add Coordinate and Civic Address based Device Location Information using EDM

Use this procedure to add local location information to the local location table for remote network devices connected to a switch or stack, based on geographical coordinates and a civic address.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Local Location** tab.
6. To add location information based on geographical coordinates for the remote device, click the **coordinateBased** cell in the LocationSubtype column for a port.
7. To add location information based on the civic address for the remote device, click the **civicAddress** cell in the LocationSubtype column for a port.
8. Click **Location Detail**.
9. Insert the local location information for the remote device.
10. Click **Ok** .
11. Click **Apply** .

#### Field Descriptions

Use the data in the following table to add coordinate-based location information for the remote device.

Name	Description
Latitude	Specifies the latitude in degrees, and its relation to the equator (North or South).
Longitude	Specifies the longitude in degrees, and its relation to the prime meridian (East or West).
Altitude	Specifies the altitude, and the units of measurement used (meters or floors).

*Table continues...*



Name	Description
Map Datum	Specifies the map reference datum. Values include: <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> </ul>

## Field Descriptions

Use the data in the following table to add civic address information for the remote device.

Name	Description
Country Code	Specifies a country using a 2 character string, example US (United States), CA (Canada), DE (Germany)
State	Specifies a state, e.g. NJ, FL
County	Specifies a county, e.g. Alameda
City	Specifies a city, e.g. Sunnyvale
City District	Specifies a city district, e.g. Santa Clara
Block (Neighborhood, block)	Specifies a block, e.g. 3
Street	Specifies a street, e.g. Great America Parkway
Leading street direction	Specifies a leading street direction, e.g. N
Trailing street suffix	Specifies a trailing street suffix, e.g. SW
Street suffix	Specifies a street suffix, e.g. Ave, Blvd
House number	Specifies a house number, e.g. 123
House number suffix	Specifies a house number suffix, e.g. A, 1/2
Landmark or vanity address	Specifies a landmark or vanity address, e.g. Columbia University
Additional location info	Example: South Wing
Name (Residence and office occupant)	Example: Joe's Barbershop
Postal/Zip code	Specifies a postal or zip code, e.g. 95054
Building (structure)	Example: Low Library
Apartment (suite)	Example: Apt 42
Floor	Example: 8
Room number	Example: 450F
Place type	Example: office
Postal community name	Example: Leonia
Post office box (P.O. Box)	Example: 12345
Additional Code	Example: 13203000003

## View Local PoE PSE Information using EDM

Use this procedure to display LLDP PoE PSE information for the local system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Local PoE PSE** tab.

### Local PoE PSE Tab Field Descriptions

Use the data in the following table to use the **Local PoE PSE** tab.

Name	Description
PortNum	Indicates the port number.
PSEPortPowerAvailable	Contains the value of the power available (in units of 0.1 watts) from the PSE through this port.
PSEPortPDPriority	Indicates the PD power priority that is advertised on this PSE port: <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>

## View Neighbor Capabilities using EDM

Use this procedure to display LLDP capabilities for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor Capabilities** tab.

### Neighbor Capabilities Tab Field Descriptions

Use the data in the following table to use the **Neighbor Capabilities** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
CapSupported	Identifies the MED system capabilities supported on the remote system.
CapCurrent	Identifies the MED system capabilities that are enabled on the remote system.
DeviceClass	Indicates the remote MED device class.

## View Neighbor Policies using EDM

Use this procedure to display LLDP policy information for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor Policy** tab.

### Neighbor Policy Tab Field Descriptions

Use the data in the following table to use the **Neighbor Policy** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
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

*Table continues...*

Name	Description
	frames, meaning that only the 802.1p priority level is significant and that the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the remote system connected to the port.
PolicyDscp	Contains the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the remote system connected to the port.
PolicyUnknown	Indicates whether the network policy for the specified application type is currently unknown or defined.
PolicyTagged	Indicates whether the application is using a tagged VLAN, untagged VLAN, or does not support a port based VLAN operation.

## Near Neighbor Location Information Management using EDM

Use the information in this section to view and add neighbor location information for network devices connected to a switch or stack.

### View Neighbor Location Information using EDM

Use this procedure to display LLDP neighbor location information.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor Location** tab.

### Neighbor Location Tab Field Descriptions

Use the data in the following table to use the **Neighbor Location** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index

*Table continues...*

Name	Description
	values to new entries, starting with one, after each reboot.
LocationSubtype	Indicates 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	Indicates the location information advertised by the remote device. The parsing of this information depends on the location subtype.

### Add Coordinate-based Neighbor Location Information using EDM

Use this procedure to add coordinate-based location information to the neighbor location table.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor Location** tab.
6. In the table, select a location with the **LocationSubtype** listed as **coordinateBased**.
7. On the toolbar, click the **Location Details** button.  
The Insert Local Location dialog box appears.
8. Click **Close** to close the dialog box.
9. Click **Apply** .

### Add Civic Address Location Information using EDM

Use this procedure to add civic address-based location information to the neighbor location table.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor Location** tab.
6. In the table, select a location with the **LocationSubtype** listed as **civicAddress**.
7. On the toolbar, click the **Location Details** button.  
The Insert Local Location dialog box appears.

8. Click **Close** to close the dialog box.
9. Click **Apply** .

## View Neighbor PoE Information using EDM

Use this procedure to display LLDP PoE properties for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor PoE** tab.

### Neighbor PoE Tab Field Descriptions

Use the data in the following table to use the **Neighbor PoE** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PoeDeviceType	Defines the type of Power-via-MDI (Power over Ethernet) advertised by the remote device: <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>

## View Neighbor PoE PSE Information using EDM

Use this procedure to display LLDP PoE PSE information for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.

4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor PoE PSE** tab.

### Neighbor PoE PSE Tab Field Descriptions

Use the data in the following table to use the **Neighbor PoE PSE** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
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. <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	Specifies the priority advertised by the PSE 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>

### View Neighbor PoE PD Information using EDM

Use this procedure to display LLDP PoE PD information for the remote system.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor PoE PD** tab.

## Neighbor PoE PD Tab Field Descriptions

Use the data in the following table to use the **Neighbor PoE PD** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
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>

## View Neighbor Inventory using EDM

Use this procedure to display LLDP inventory information for the remote system.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. On the work area, click the **Neighbor Inventory** tab.



## Neighbor Inventory Tab Field Descriptions

Use the data in the following table to use the **Neighbor Inventory** tab.

Name	Description
TimeMark	Indicates the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Indicates the arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
HardwareRev	Indicates the vendor-specific hardware revision string as advertised by the remote device.
FirmwareRev	Indicates the vendor-specific firmware revision string as advertised by the remote device.
SoftwareRev	Indicates the vendor-specific software revision string as advertised by the remote device.
SerialNum	Indicates the vendor-specific serial number as advertised by the remote device.
MfgName	Indicates the vendor-specific manufacturer name as advertised by the remote device.
ModelName	Indicates the vendor-specific model name as advertised by the remote device.
AssetID	Indicates the vendor-specific asset tracking identifier as advertised by the remote device.

# Chapter 7: Zero Touch Provisioning Plus (ZTP+)

This chapter provides conceptual and procedural information to configure and manage Zero Touch Provisioning Plus (ZTP+).

---

## ZTP+ Fundamentals

---

### ZTP+

Using ZTP+, switches communicate with the Extreme Management Center (XMC) as soon as they are connected to the network, allowing them to obtain firmware and configuration updates automatically. This auto-provisioning process significantly minimizes the amount of time required to configure a new switch and deploy it on the network.

 **Note:**

ZTP+ is compatible only with XMC version 8.4.0.0 or later.

ZTP+ is enabled by default on the switch and is intended only for the initial provisioning of newly deployed switches with no prior configuration. It does not replace traditional provisioning options such as CLI or SNMP, which are required to further set up the switch as intended, to operate within the network. After the ZTP+ provisioning completes, it is automatically disabled on the switch. You can re-enable ZTP+, but the process starts only after a system reboot.

ZTP+ uses HTTPS for communication between the switch and the XMC server.

ZTP+ supports use of both the In Band and Out of Band Management interface for connection to the XMC server.

As part of the ZTP support, DHCP for the Out of Band Management client support was added. For more information on configuring a DHCP client for the Out of Band Management interface, see [DHCP-OOB client](#) on page 451.

## DHCP-OOB client

The DHCP client for the OOB interface (DHCP-OOB) supports ZTP+ onboarding and auto-provisioning over the OOB interface. DHCP-OOB requires an available Dynamic Host Configuration Protocol (DHCP) server on the network.

This feature assigns an IPv4 address, subnet mask, default gateway, Domain Name Server (DNS), and Domain Name (DN) information on the Base Unit (BU) of a stack or a standalone switch.

By default, DHCP-OOB is enabled and the BootP state is set to dhcp-when-needed. The switch will receive information from the DHCP server like IPv4 address, subnet mask, default gateway, DNS and DN.

When DHCP-OOB is disabled, the BootP state is set to dhcp-disabled. No information is retrieved from the DHCP server. IP management address is restored as 0.0.0.0.

### \* Note:

DHCP client functionality on the OOB interface was mainly added to support ZTP+ onboarding and auto provisioning over the same interface. Therefore, DHCP-OOB has the following limitations:

- DHCP-OOB feature is not used if the management port is down or has no link since there is no communication with the DHCP server.
- In stack mode, the DHCP-OOB task runs only on the Base Unit.
- The DHCP-OOB feature does not have support for the "Lease" in IP management address allocation.
- Temporary Base Unit scenario is not supported; the device does not request another IP address when the Base Unit fails.
- DNS and domain name are set either through DHCP or statically with no priority; the last configured one remaining active.

---

## ZTP+ Phases of Operation

ZTP+ auto-provisioning happens in phases after you connect the switch to the network. After the process completes, ZTP+ is disabled on the switch.

In the case of a stack, when a switch is added to a stack that is already ZTP+ provisioned and has ZTP+ disabled on it (because the process completed successfully), the updated stack continues to be in the ZTP+ provisioned state with ZTP+ disabled.

### \* Note:

Regarding the ZTP+ communication between the device and the XMC server, because there can be an In Band interface as well as an Out of Band interface configured on the device, the recommendation is to use only one of them. Also, ensure that the appropriate **Management interface** is selected in XMC when configuring the device.

## Connect

The Connect phase is the first phase of ZTP+ during which the switch connects to the XMC server on the network.

To facilitate connectivity, you must first configure a domain name for the XMC server on the network. You can either choose the default domain name: *extremecontrol*, or configure a custom domain name and then map *extremecontrol.<customDomainName>* to the XMC server. A DNS server on the network enables the switch to obtain the IP address of the XMC server using the domain name. You can also configure a DHCP server on the network to obtain a dynamic DHCP lease for network connectivity between the switch and the XMC server.

The switch attempts to connect to the XMC server in the following order:

- *extremecontrol*
- *extremecontrol.<customDomainName>*

If the attempt is successful, the XMC server responds with an **Accept** message.

Once connectivity is established, the switch communicates with the XMC server securely and transmits information such as its serial number, MAC address, and other parameters such as the Ethernet speed and negotiation capabilities. The switch then progresses to the next phase of ZTP+.

## Firmware Validation

After a successful connect to the XMC server, the next phase of ZTP+ is firmware validation. This phase verifies that the switch is running the firmware version that is currently selected as the **reference** version on the XMC server.

Firmware validation is initiated by the switch. After a successful connect, the switch sends an image update request to the XMC server with details on the current firmware version. If the firmware versions on the switch and the XMC server match, no update is initiated, and the switch moves to the next phase of ZTP+. If the XMC detects a different firmware version, the firmware is automatically pushed to the switch. In the case of a switch stack, the firmware is pushed to all switches in the stack.

### Important:

For the duration of the firmware update (typically 10 to 15 minutes on an 8-unit stack), you cannot perform any configuration on the switch.

After a successful firmware update, the switch reboots and reconnects to the XMC server. If there are errors in the firmware update process, the switch retries the firmware update.

## Configuration

The next phase after firmware validation is ZTP+ configuration or auto-provisioning. During this phase, the switch queries the XMC server for configuration updates, and initiates auto-provisioning by transmitting information about itself, such as the image version, model name, and serial number. The switch then attempts to apply the configuration that is pushed from the XMC server.

You can configure the following on the XMC server to be pushed to the switch.

### Device settings for the switch:

- IP configuration, which includes:
  - the switch IP address and subnet

**\* Note:**

You can either retain the IP address discovered by the switch using DHCP (with IP and management interface discovery enabled) or configure a different IP address (with IP discovery disabled).

- the IP address of the default router (default gateway)
- the IP addresses of the configured DNS servers (up to three)
- Custom domain name (maximum of 255 characters in length)

**User Configuration:**

- User log in information: The supported range for user name length is 2 to 16 characters. The password must be AAA compliant.
- System contact (maximum of 255 characters in length)
- System location (maximum of 255 characters in length)
- System name (maximum of 255 characters in length)

**VLAN Configuration:**

- VLAN creation: You can configure a maximum of 1024 VLANs.
- VLAN modification: You can modify the names of existing VLANs. The supported maximum length of a VLAN name is 16 characters.

**Port Configuration:**

- Enabling or disabling of the administrative status of ports.
- Configuration of a port alias; The maximum supported length of the interface name is 64 characters.
- Configuration of auto-negotiation settings.

**\* Note:**

Configuration of VLAN port membership is not supported

**\* Note:**

No configuration can be set for the Out of Band Management port.

**LLDP Configuration:**

This includes only LLDP neighbor discovery and not enabling or disabling LLDP. Based on the LLDP neighbor discovery, port templates can be used on the XMC.

**SNMP Configuration:**

- Configuration of SNMPv1/SNMPv2 community strings, with a maximum of 32 characters.
- Configuration of SNMPv3 user name and password, with a maximum of 32 characters.

If the switch fails to apply the configuration received, an event is added to the server log.

To aid auto-provisioning, you can preregister the switch with the XMC server. For more information on how to preregister the switch on the XMC, see the XMC documentation.

---

## ZTP+ Limitations

The switch does not support the configuration of any other feature using ZTP+ that is not listed as supported.

---

## Configuring ZTP+ using the CLI

This section provides procedures to configure and manage ZTP+ using the Command Line Interface (CLI).

---

### View ZTP+ Status

#### About this task

Use this procedure to verify the status of ZTP+ on the switch.

#### Procedure

1. To enter User EXEC mode, log on to the switch.
2. Verify that ZTP+ is enabled:

```
show auto-provision
```

#### Example

The following is an example output of the `show auto-provision` command:

```
Switch:1>show auto-provision
Admin state       : Enabled
Operational state : Running
```

---

### Enable ZTP+

#### About this task

ZTP+ is enabled on the switch by default, and is automatically disabled after the auto-provisioning process completes. You can however re-enable ZTP+ using this procedure.

- \* **Note:**  
ZTP+ is re-enabled only after a switch reboot.

#### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

## 2. Enable ZTP+ auto-provisioning:

```
auto-provision enable
```

### Example

The following example enables ZTP+ auto-provisioning and verifies the configuration.

```
Switch:1>en
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch:1(config)#auto-provision enable
```

Verify that ZTP+ is enabled:

```
Switch:1(config)#show auto-provision

Admin state      : Enabled
Operational State : Not running
```

---

## Disable ZTP+

### About this task

ZTP+ is enabled on the switch by default. Use this procedure to disable ZTP+.

- \* Note:**  
ZTP+ is disabled only after a switch reboot.

### Procedure

#### 1. Enter Global Configuration mode:

```
enable
configure terminal
```

#### 2. Disable ZTP+ auto-provisioning:

```
no auto-provision enable
```

### Example

The following example disables ZTP+ auto-provisioning and verifies the configuration.

```
Switch:1>en
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch:1(config)#no auto-provision enable
```

Verify that ZTP+ is enabled:

```
Switch:1(config)#show auto-provision
```

```
Admin state      : Disabled
Operational State : Not running
```

---

## Verify the Firmware Version

### About this task

Verify the firmware version pushed to the switch using ZTP+.

### Procedure

1. To enter User EXEC mode, log on to the switch.
2. Verify the version of firmware pushed to the switch:

```
show boot
```

### Example

The following example verifies the version of firmware pushed to the switch:

```
Switch:1>show boot

Unit  Agent Image Secondary Image Active Image Diag Image Active Diag
-----
1     7.8.0.021  7.5.0.053      7.8.0.021   7.4.0.8    7.4.0.8
* - Unit requires reboot for new Active Image to be made operational.
# - Unit requires reboot for new Diag to be made operational.
```

---

## Verify DNS Configuration

### About this task

Verify DNS configuration on the switch.

The switch uses DNS server(s) to obtain the *extremecontrol* (XMC server) IP address. You can configure up to three DNS servers on the network.

### Procedure

1. To enter User EXEC mode, log on to the switch.
2. View DNS configuration:

```
show ip dns
```

### Example

The following example verifies DNS configuration on the switch:

```
Switch:1>show ip dns

DNS Default Domain name: default.domainname.com

DNS Servers
-----
172.30.201.5
```



```
172.30.201.4
0.0.0.0
```

## Verify ZTP+ Auto-provisioning

### Procedure

1. Enter Privileged EXEC mode:
 

```
enable
```
2. Verify ZTP+ auto-provisioning:
  - View VLAN configuration: `show vlan`
  - View SNMP users: `show snmp-server user`
  - View interface status and configuration: `show interfaces`
  - View auto-negotiation advertisement: `show auto-negotiation-capabilities`
  - View user roles and log-in permissions:
 

```
show username
```
  - View LLDP neighbor information: `show lldp neighbor`

### Example

Use the following sections to verify ZTP+ auto-provisioning on the switch.

View VLAN configuration:

```
Switch:1#show vlan
```

Id	Name	Type	Protocol	PID	Active	IVL/SVL	Mgmt
1	VLAN #1 Port Members: ALL	Port	None	0x0000	Yes	IVL	Yes
100	VLAN #100 Port Members: NONE	Port	None	0x0000	Yes	IVL	No
200	VLAN #200 Port Members: NONE	Port	None	0x0000	Yes	IVL	No

```
Total VLANs: 3
```

View SNMP user configuration:

```
Switch:1#show snmp-server user
```

```
User Name: v3-user
SNMP Engine ID: 80:00:02:32:80:02:00:51:58:4C:49:52:37:32:34:54:32:31:30:30:30:38
Authentication Protocol: MD5
Privacy Protocol: AES
Storage Type: Non Volatile(NVRAM)
Status: Active
Views for Unauthenticated Access:
Read View:
Write View:
Notify View:
Views for Authenticated Access:
Read View:
Write View:
Notify View:
```

## Zero Touch Provisioning Plus (ZTP+)

```
Views for Authenticated and Encrypted Access:
Read View:
Write View:
Notify View:
```

### View interface status and configuration:

```
Switch:1#show interfaces
```

Port	Trunk	Status		Link	LinkTrap	Auto Negotiation	Speed	Duplex	Flow Control
		Admin	Oper						
1		Enable	Up	Up	Enabled	Enabled	100Mbps	Full	Disable
2		Enable	Up	Up	Enabled	Enabled	1000Mbps	Full	Asymm
3		Enable	Down	Down	Enabled	Disabled	10Gbps	Full	Asymm
4		Enable	Down	Down	Enabled	Disabled	10Gbps	Full	Asymm
5		Enable	Down	Down	Enabled	Disabled	10Gbps	Full	Asymm

### View auto-negotiation advertisement capabilities for the ports.

```
Switch:1#show auto-negotiation-capabilities
```

Port	Autonegotiation Capabilities					
1	10Full	10Half	100Full	100Half	1000Full	AsymmPause
2	10Full	10Half	100Full	100Half	1000Full	AsymmPause
3	10Full	10Half	100Full	100Half	1000Full	AsymmPause

### View user roles and log-in permissions:

```
Switch:1#show username
```

```
Lockout timeout: 1 min
Lockout retries: 0
```

```
Username: RW
-----
Role name: RW
Enabled: Yes
Password aging-time: 0 days
Password expired: No
Lockout status: Available
Inactive period: 0 days
SSH access: Enabled
TELNET access: Enabled
```

```
Username: RO
-----
Role name: RO
Enabled: Yes
Password aging-time: 0 days
Password expired: No
Lockout status: Available
Inactive period: 0 days
SSH access: Enabled
TELNET access: Enabled
```

### View LLDP neighbor information:

```
Switch:1#show lldp neighbor
```

```
-----
LLDP neighbor
-----
Port: 2      Index: 1      Time: 0 days, 00:01:37
```

```
ChassisId: MAC address      00:1c:9c:66:94:00
PortId:    MAC address      00:1c:9c:66:94:04
-----
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 1
```

---

## Enable the DHCP-OOB client

### About this task

Use this procedure to enable the DHCP-OOB client.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. Enable the DHCP-OOB client:  
`ip mgmt address source dhcp-when-needed`
3. Press Enter.

---

## Disable the DHCP-OOB client

### About this task

Use this procedure to disable the DHCP-OOB client.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. Disable the DHCP-OOB client:  
`ip mgmt address source configured-address`
3. Press Enter.

---

## Verify IP Settings

### About this task

Use this procedure to verify the current IP settings.

## Procedure

1. Enter Global Configuration mode:  
enable  
configure terminal
2. View the current DHCP mode.  
show ip mgmt address source
3. View the current Management IP settings.  
show ip mgmt
4. View the current IP settings.  
show ip

## Example

```
4926GTS-PWR+(config)#show ip mgmt address source
DHCP Mode: DHCP When Needed

4926GTS-PWR+(config)#show ip mgmt
Configured In Use Last BootP/DHCP
-----
Mgmt Stack IP Address: 0.0.0.0
Mgmt Switch IP Address: 90.90.91.129 90.90.91.129
Mgmt Subnet Mask: 255.255.255.0 255.255.255.0
Mgmt Def Gateway: 90.90.91.1 90.90.91.1
-----

4926GTS-PWR+(config)#show ip
Bootp/DHCP Mode: BootP Or DHCP Or Default IP
Configured In Use Last BootP/DHCP
-----
Stack IP Address: 192.168.1.2 0.0.0.0
Switch IP Address: 192.168.1.1 90.90.74.240
Switch Subnet Mask: 255.255.255.0 255.255.255.0 255.255.255.0
Mgmt Stack IP Address: 0.0.0.0
Mgmt Switch IP Address: 90.90.91.129 90.90.91.129
Mgmt Subnet Mask: 255.255.255.0 255.255.255.0
Mgmt Def Gateway: 90.90.91.1 90.90.91.1
Default Gateway: 0.0.0.0 90.90.74.1
```

---

## Configuring ZTP+ Examples

---

### Configure and Manage a Simple ZTP+ Solution

#### Before you begin

- Ensure that the switch is ZTP+ enabled. ZTP+ is enabled by default.

- If you use switches in stacking configuration, ensure that you set up the switch stack first before ZTP+ provisioning.
- Ensure that the switch (or stack) runs the current version of software and is reset to factory default configuration. If running an earlier version, download the current version with the `no-reset` parameter. Then, use the `boot` command to restore the switch (or stack) to factory default settings after the reboot.
- Ensure that the XMC server is running software version 8.4.0.0 or later.
- Configure a domain name for the XMC server instance on the network. You can either choose the default domain name: *extremecontrol*, or configure a custom domain name and then map *extremecontrol.<customDomainName>* to the XMC server.
- Configure a DHCP server on the network, so that the switch can receive a dynamic DHCP lease for network connectivity between the switch and the XMC server.
- Configure a DNS server on the network to enable the switch to obtain the IP address of the XMC server, based on the configured domain name.

### About this task

The following sections describes a ZTP+ solution in its simplest form to manage auto-provisioning. At the heart of this solution is the ZTP+ enabled switch, which on successfully connecting to the XMC server, automatically updates its firmware version and auto-provisions itself with configuration pushed from the XMC server.

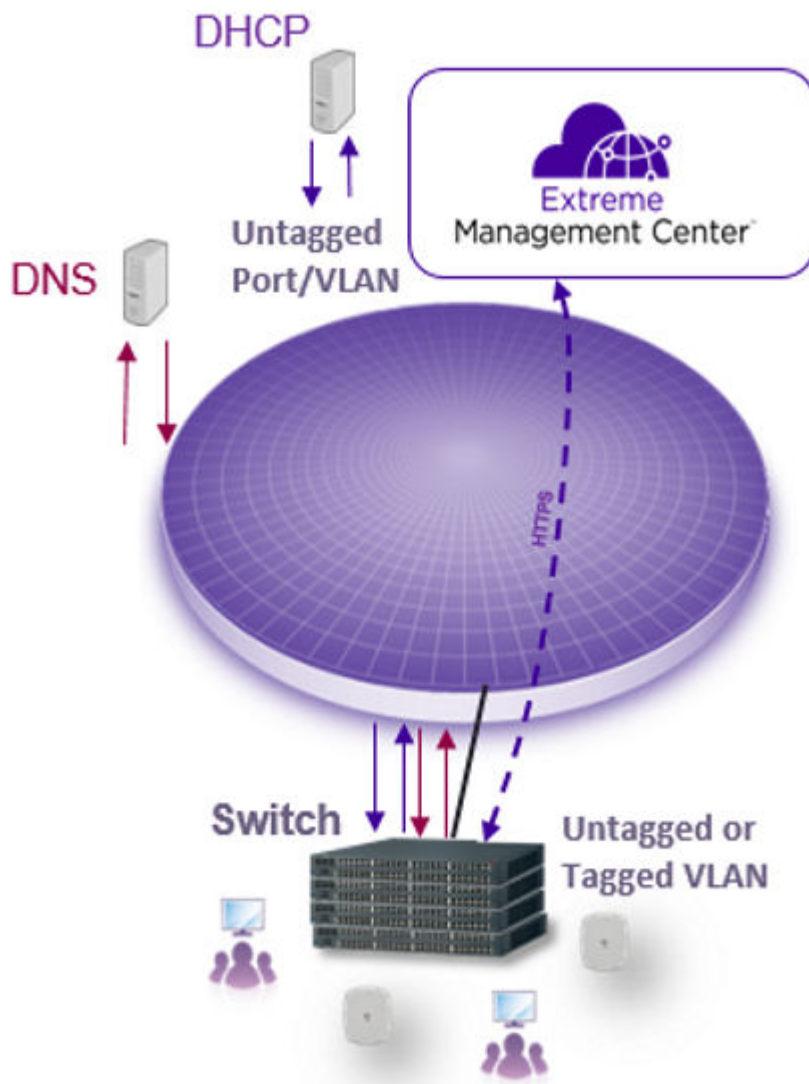


Figure 16: A simple ZTP+ solution

### Procedure

1. Verify that the switch is enabled for ZTP+ auto-provisioning:  
`show auto-provision`
2. Connect the switch to the network.
3. Verify DNS configuration on the switch.

Verify that the switch obtains the correct IP address and subnet mask, the IP address of the default router (default gateway) and those of the configured DNS servers. Verify also that the switch obtains the correct domain name.

```
show ip
show ip dns
```

4. **(Optional)** Preregister the switch with the XMC server.

This is however not mandatory for the switch to connect to and be discovered by the XMC server.

5. Verify that the switch successfully connects to the XMC server.

View the switch log: `show logging`

On the XMC server, verify that the switch is successfully discovered.

**\* Note:**

If the XMC server does not discover the switch, verify:

- the settings obtained from the DHCP server.
- that the XMC server (*extremecontrol* or *extremecontrol.<customDomainName>*) is reachable using the `ping` command.
- that the switch is not previously registered with the XMC server, for example, with its serial number. Determine this by viewing the XMC server log. The following text is an example of the log message if the switch is already registered:

```
"ERROR
[com.enterasys.netsight.server.webapps.monitor.ezConfig.MsgDispatcher] ZTP
+ 90.90.74.241 is connecting but already in the database with ezconfig flag
as false and poller type set to SNMP"
```

6. Update the reference firmware image on the XMC server, which is the firmware version to be pushed to the switch using ZTP+.

You need to first upload the firmware image and then set it as the reference image. When you upload the image, also configure the appropriate file transfer mode to the switch. The switch supports both the TFTP and the SFTP file transfer modes. TFTP is the default mode.

7. Verify that the switch is updated with the firmware image selected as the reference image on the XMC server:

**\* Note:**

An update is initiated only if the image configured on the switch is different from the reference image on the XMC server.

After the firmware update, the switch reboots and reconnects to the XMC server.

`show boot`

View the switch log: `show logging`

8. Verify that the switch reconnects with the XMC server, after the reboot:

`show auto-provision`

View the switch log: `show logging`

On the XMC server, view the status of the switch. After a successful reconnect, the switch is discovered with a status of **ZTP+ Pending Edit**.

At this stage, the switch is ready for ZTP+ auto-provisioning.

9. On the XMC server, as part of switch (device) configuration, perform the following configuration to be pushed to the switch using ZTP+. Save the configuration.
  - **IP configuration:** Includes the switch IP address and subnet, the IP address of the default gateway, the IP addresses of the DNS servers (up to three) and a custom domain name.

**\* Note:**

You can either retain the IP address discovered by the switch using DHCP (with IP and management interface discovery enabled) or configure a different IP address (with IP discovery disabled).

- **User configuration:** Includes user login information, system name, system contact and system location.
- **VLAN configuration:** Includes either the configuration of new VLANs or modifying the names of existing VLANs.
- **Port configuration:** Includes enabling or disable the administrative status of ports, configuring a port alias or auto-negotiation settings.
- **SNMP configuration:** Includes the configuration of SNMPv1/SNMPv2 community strings and/or SNMPv3 user name and password settings.
- **LLDP configuration:** Includes neighbor discovery only. Also, based on the LLDP neighbor discovery, port templates can be used on the XMC.

For more information on the actual configuration steps on the XMC server, see the *Extreme Management Center User Guide* for XMC version 8.4.0.0 or later.

After you save the configuration, auto-provisioning of the switch begins and the XMC server displays the switch status as **ZTP+ Staged**.

After the auto-provisioning successfully completes, the switch status changes to **ZTP+ Complete**. Also, the switch console displays a log that corresponds to the acknowledgment received from the XMC server on successful auto-provisioning.

10. Verify ZTP+ auto-provisioning on the switch:

View the switch log: `show logging`.

Verify the switch configuration in detail:

- View the consolidated system information (to verify the configured system name, system contact and system location):

```
show system
```

```
show sys-info
```

- View IP configuration:

```
show ip
```



- View VLAN configuration: `show vlan`
- View SNMP users: `show snmp-server user`
- View interface status and configuration: `show interfaces`
- View auto-negotiation advertisement: `show auto-negotiation-capabilities`
- View user roles and log-in permissions:  
`show username`
- View LLDP neighbor information: `show lldp neighbor`

On the XMC server, verify the status of auto-provisioning by checking the ZTP+ event log.

11. Verify that ZTP+ is disabled on the switch after successful auto-provisioning.

```
show auto-provision
```

### Example

Verify that the switch is enabled for ZTP+ auto-provisioning:

```
Switch:1>show auto-provision
```

```
Admin state      : Enabled
Operational state : Running
```

Connect the switch to the network.

Verify DNS configuration on the switch.

```
Switch:1>show ip dns
DNS Default Domain name: default.domainname.com
```

```
DNS Servers
-----
172.30.201.5
172.30.201.4
0.0.0.0
```

Optionally, preregister the switch with the XMC server.

Verify that the switch successfully connects to the XMC server; View the switch log. On the XMC server, verify that the switch is successfully discovered.

```
Switch:1#show logging
...
...
I      2008-09-17T21:20:09+00:00      5      successfully connected to the XMC server
...
...
```

Update the reference firmware image on the XMC server, which is the firmware version to be pushed to the switch using ZTP+. First upload the firmware image and then set it as the reference image. Also configure the file transfer mode as TFTP or SFTP.

Verify that the switch is updated with the firmware image selected as the reference image on the XMC server:

**\* Note:**

An update is initiated only if the image configured on the switch is different from the reference image on the XMC server.

After the firmware update, the switch reboots and reconnects to the XMC server.

```
Switch:1>show boot

Unit  Agent Image Secondary Image Active Image Diag Image Active Diag
-----
1      7.8.0.021  7.5.0.053      7.8.0.021  7.4.0.8  7.4.0.8
* - Unit requires reboot for new Active Image to be made operational.
# - Unit requires reboot for new Diag to be made operational.
```

View the switch log to view the status of the firmware update:

```
Switch:1#show logging
...
...
I      2008-09-17T21:20:09+00:00  4      successfully connected to the XMC server
I      2008-09-17T21:20:09+00:00  5      the firmware upgrade has started
I      2008-09-17T21:20:09+00:00  5      successfully upgraded the firmware
...
...
```

Verify that the switch reconnects with the XMC server, after the reboot.

```
Switch:1#show logging
...
...
I      2008-09-17T21:20:09+00:00  4      successfully connected to the XMC server
...
...
```

```
Switch:1>show auto-provision
```

```
Admin state      : Enabled
Operational state : Running
```

On the XMC server, view the status of the switch. After a successful reconnect, the switch is discovered with a status of **ZTP+ Pending Edit**. At this stage, the switch is ready for ZTP+ auto-provisioning.

As part of device configuration on the XMC server, configure the following to be pushed to the switch. Save the configuration.

- IP configuration
- User configuration
- VLAN configuration
- Port configuration:
- SNMP configuration
- LLDP configuration

After the configuration is saved, auto-provisioning of the switch begins and the XMC server displays the switch status as **ZTP+ Staged**.

After the auto-provisioning successfully completes, the switch status changes to **ZTP+ Complete**. Also, the switch console displays a log that corresponds to the acknowledgment received from the XMC server on successful auto-provisioning.

## View ZTP+ auto-provisioning of the switch:

```
Switch:1#show logging
...
...
I    2008-09-17T21:20:09+00:00    4    successfully connected to the XMC server
I    2008-09-17T21:20:09+00:00    5    the firmware upgrade has started
I    2008-09-17T21:20:09+00:00    5    successfully upgraded the firmware
I    2008-09-17T21:20:09+00:00    4    the auto-provisioning process has started
...
...
```

## Verify ZTP+ auto-provisioning in detail:

- View the consolidated system information (to verify the configured system name, system contact and system location):

```
Switch:1#show system

System Information:
  Operation Mode:      Switch
  MAC Address:        00-1B-4F-F9-70-00
  PoE Module FW:      1.5.0.11
  Reset Count:        155
  Last Reset Type:    Software Download
  Autotopology:       Enabled
  Base Unit Selection: Non-base unit using rear-panel switch
  sysDescr:           Ethernet Routing Switch 5952GTS-PWR+
                      HW:ROD.7    FW:7.4.0.8    SW:v7.8.0.093
  sysObjectID:        1.3.6.1.4.1.45.3.81.4
  sysUpTime:          9 days, 14:01:04
  sysNtpTime:         NTP not synchronized.
  sysRtcTime:         Tuesday 2020/01/09 16:52:56
  sysServices:        6
  sysContact:
  sysName:            Test switch
  sysLocation:
  Stack sysAssetId:
  Operational license: Base Software
  Installed license:  Base Software
```

```
Switch:1#show sys-info

Operation Mode:      Switch
Enhanced Secure Mode: Disabled
MAC Address:        00-1B-4F-F9-70-00
PoE Module FW:      1.5.0.11
Reset Count:        155
Last Reset Type:    Software Download
Power Supply 1:     Unavailable
Power Supply 2:     AC-DC-56V1400W-F2B
Power Status :      1- Not Present 2- OK
Autotopology:       Enabled
Pluggable Port 49:  None
Pluggable Port 50:  None
Pluggable Port 51:  None
Pluggable Port 52:  None
Base Unit Selection: Non-base unit using rear-panel switch
sysDescr:           Ethernet Routing Switch 5952GTS-PWR+
                      HW:ROD.7    FW:7.4.0.8    SW:v7.8.0.093
Mfg Date:20140712    HW Dev:none
Serial #:           XLIR748P310006
Operational Software: FW:7.4.0.8    SW:v7.8.0.093
Installed software:  FW:7.4.0.8    SW:v7.8.0.093
```

## Zero Touch Provisioning Plus (ZTP+)

```
Operational license: Base Software
Installed license: Base Software
sysObjectID: 1.3.6.1.4.1.45.3.81.4
sysUpTime: 9 days, 14:07:52
sysNtpTime: NTP not synchronized.
sysRtcTime: Tuesday 2009/06/09 16:59:48
sysServices: 6
sysContact:
sysName:
sysLocation:
Stack sysAssetId:
Unit sysAssetId:
```

- **View IP configuration:**

```
Switch:1#show ip
```

```
Bootp/DHCP Mode: BootP Or DHCP Or Default IP
```

	Configured	In Use	Last BootP/DHCP
Stack IP Address:	198.51.100.2		0.0.0.0
Switch IP Address:	192.0.22.162	192.0.22.162	0.0.0.0
Switch Subnet Mask:	255.255.255.0	255.255.255.0	0.0.0.0
Mgmt Stack IP Address:	0.0.0.0		
Mgmt Switch IP Address:	0.0.0.0		
Mgmt Subnet Mask:	255.255.255.0		
Mgmt Def Gateway:	1.2.3.4		
Default Gateway:	203.0.113.0	203.0.113.0	0.0.0.0

- **View VLAN configuration:**

```
Switch:1#show vlan
```

Id	Name	Type	Protocol	PID	Active	IVL/SVL	Mgmt
1	VLAN #1	Port	None	0x0000	Yes	IVL	Yes
	Port Members: ALL						
100	VLAN #100	Port	None	0x0000	Yes	IVL	No
	Port Members: NONE						

Total VLANs: 2

- **View SNMP user configuration:**

```
Switch:1#show snmp-server user
```

```
User Name: v3-user
SNMP Engine ID: 80:00:02:32:80:02:00:51:58:4C:49:52:37:32:34:54:32:31:30:30:30:38
Authentication Protocol: MD5
Privacy Protocol: AES
Storage Type: Non Volatile(NVRAM)
Status: Active
Views for Unauthenticated Access:
Read View:
Write View:
Notify View:
Views for Authenticated Access:
Read View:
Write View:
Notify View:
Views for Authenticated and Encrypted Access:
Read View:
Write View:
Notify View:
```

- View interface (port) status and configuration:

```
Switch:1#show interfaces
```

Port	Trunk	Admin	Oper	Link	LinkTrap	Auto Negotiation	Speed	Duplex	Flow Control
1		Enable	Up	Up	Enabled	Enabled	100Mbps	Full	Disable
2		Enable	Up	Up	Enabled	Enabled	1000Mbps	Full	Asymm

#### View auto-negotiation advertisement capabilities for the ports.

```
Switch:1#show auto-negotiation-capabilities
```

Port	Autonegotiation	Capabilities
1	10Full 10Half 100Full 100Half 1000Full	AsymmPause
2	10Full 10Half 100Full 100Half 1000Full	AsymmPause
3	10Full 10Half 100Full 100Half 1000Full	AsymmPause

- View user roles and log-in permissions:

```
Switch:1#show username
```

Lockout timeout: 1 min  
Lockout retries: 0

Username: RW

---

Role name: RW  
Enabled: Yes  
Password aging-time: 0 days  
Password expired: No  
Lockout status: Available  
Inactive period: 0 days  
SSH access: Enabled  
TELNET access: Enabled

Username: RO

---

Role name: RO  
Enabled: Yes  
Password aging-time: 0 days  
Password expired: No  
Lockout status: Available  
Inactive period: 0 days  
SSH access: Enabled  
TELNET access: Enabled

- View LLDP neighbor information:

```
Switch:1#show lldp neighbor
```

LLDP neighbor			
Port: 2	Index: 1	Time: 0 days, 00:01:37	
	ChassisId: MAC address	00:1c:9c:66:94:00	
	PortId: MAC address	00:1c:9c:66:94:04	

Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router; T-Telephone; D-DOCSIS cable device; S-Station only.  
Total neighbors: 1

Verify that ZTP+ is disabled on the switch, after successful auto-provisioning.

```
Switch:1>show auto-provision
```

```
Admin state      : Disabled  
Operational state : Completed
```

---

## Configure ZTP+ with FA-Provisioned Management VLAN

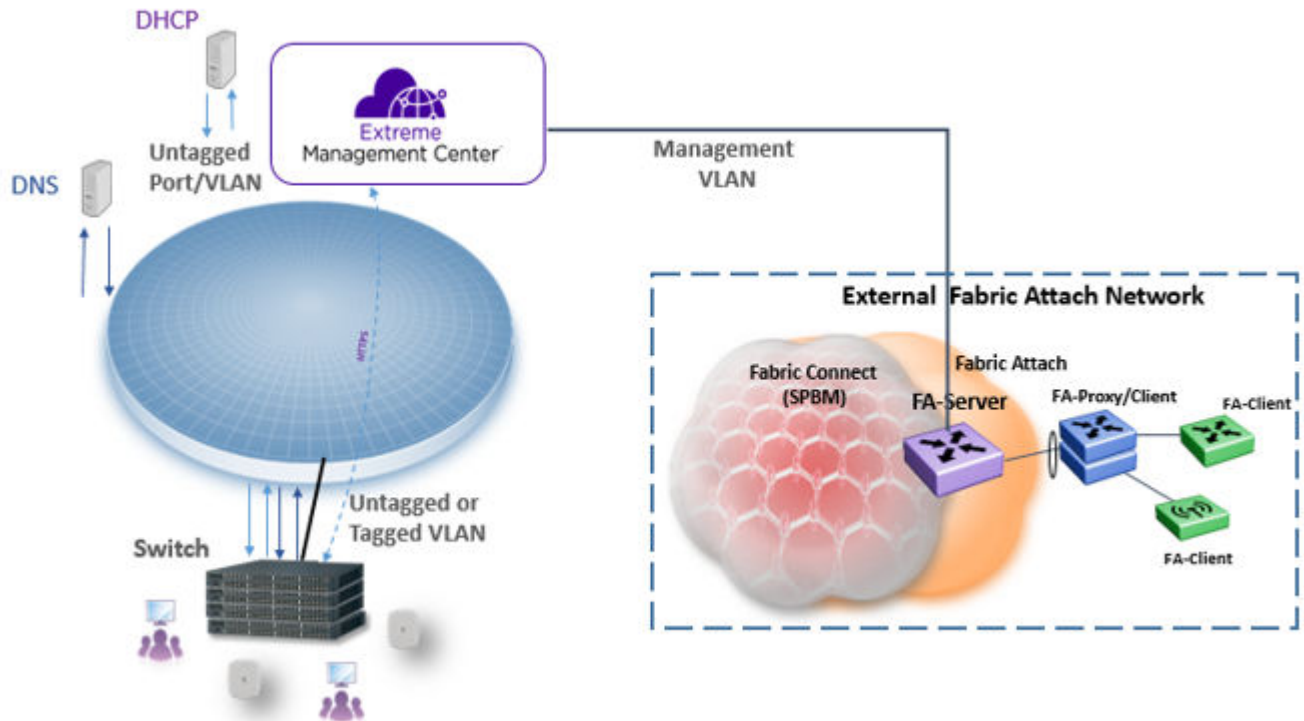
### Before you begin

- Ensure that the switch is ZTP+ enabled. ZTP+ is enabled by default.
- If you use switches in stacking configuration, ensure that you set up the switch stack first before ZTP+ provisioning.
- Ensure that the switch (or stack) runs the current version of software and is reset to factory default configuration. If running an earlier version, download the current version with the `no-reset` parameter. Then, use the `boot` command to restore the switch (or stack) to factory default settings after the reboot.
- Ensure that the XMC server is running software version 8.4.0.0 or later.
- Configure a domain name for the XMC server instance on the network. You can either choose the default domain name: *extremecontrol*, or configure a custom domain name and then map *extremecontrol.<customDomainName>* to the XMC server.
- Configure a DHCP server on the network, so that the switch can receive a dynamic DHCP lease for network connectivity between the switch and the XMC server.
- Configure a DNS server on the network to enable the switch to obtain the IP address of the XMC server, based on the configured domain name.

### About this task

On the XMC server, you can configure a non-default VLAN as the management VLAN. However, this configuration cannot be pushed to the switch using ZTP+; it is not supported. As an alternative, you can push the management VLAN from an FA server.

The following sections describes configuring a ZTP+ solution with an FA-provisioned management VLAN. At the heart of this solution is the ZTP+ enabled switch, which on successfully connecting to the XMC server, automatically updates its firmware version and auto-provisions itself with configuration pushed from the XMC server.



## Procedure

1. Verify that the switch is enabled for ZTP+ auto-provisioning:

```
show auto-provision
```

2. Connect the switch to the FA server on the network.
3. Verify DNS configuration on the switch.

Verify that the switch obtains the correct IP address and subnet mask, the correct default router (default gateway) IP address, the configured DNS servers and the domain name.

```
show ip dns
```

4. Enable FA on the switch port that connects to the FA server. Verify the configuration.

```
fa port-enable
```

```
show fa port-enable enabled-port
```

5. Configure a management VLAN on the port.

```
fa management i-sid <i-sid> <c-vid>
```

6. Verify that the switch receives the management VLAN from the FA Server.

```
show vlan mgmt
```

```
show running-config module vlan
```

7. Verify that the switch obtains an IP address in the current management VLAN from the DHCP server.

```
show ip
```

8. **(Optional)** Preregister the switch with the XMC server.

This is however not mandatory for the switch to connect to and be discovered by the XMC server.

9. Verify that the switch connects to and is discovered by the XMC server.

View the switch log: `show logging`

On the XMC server, verify that the switch is successfully discovered.

**\* Note:**

If the XMC server does not discover the switch, verify:

- the settings obtained from the DHCP server.
- that the XMC server (*extremecontrol* or *extremecontrol.<customDomainName>*) is reachable using the `ping` command.
- that the switch is not previously registered with the XMC server, for example, with its serial number. Determine this by viewing the XMC server log. The following text is an example of the log message if the switch is already registered:

```
"ERROR
[com.enterasys.netsight.server.webapps.monitor.ezConfig.MsgDispatcher] ZTP
+ 90.90.74.241 is connecting but already in the database with ezconfig flag
as false and poller type set to SNMP"
```

10. Update the reference firmware image on the XMC server, which is the firmware version to be pushed to the switch using ZTP+.

You need to first upload the firmware image and then set it as the reference image. When you upload the image, also configure the appropriate file transfer mode to the switch. The switch supports both the TFTP and the SFTP file transfer modes. TFTP is the default mode.

11. Verify that the switch is updated with the firmware image selected as the reference image on the XMC server:

**\* Note:**

An update is initiated only if the image configured on the switch is different from the reference image on the XMC server.

After the firmware update, the switch reboots and reconnects to the XMC server.

```
show boot
```

View the switch log: `show logging`

12. Verify that the switch reconnects with the XMC server, after the reboot:

```
show auto-provision
```

View the switch log: `show logging`



On the XMC server, view the status of the switch. After a successful reconnect, the switch is discovered with a status of **ZTP+ Pending Edit**.

At this stage, the switch is ready for ZTP+ auto-provisioning.

13. On the XMC server, as part of device configuration for the switch, perform the following configuration to be pushed to the switch using ZTP+ Save the configuration.

- **Management VLAN configuration:**

-  **Note:**

Since the switch does not support the configuration of a management VLAN using ZTP+, you must configure the management VLAN pushed from the FA server as the management interface, on the XMC server.

- **IP configuration:** Includes configuration of the switch IP address and subnet, the IP address of the default gateway, the IP addresses of the DNS servers (up to three) and a custom domain name
- **User configuration:** Includes user login information, system name, system contact and system location.
- **VLAN configuration:** Includes configuration of new VLANs or modifying the names of existing VLANs.
- **Port configuration:** Includes enabling or disable the administrative status of ports, configuring a port alias or auto-negotiation settings.
- **SNMP configuration:** Includes the configuration of SNMPv1/SNMPv2 community strings and/or SNMPv3 user name and password settings.
- **LLDP configuration:** Includes neighbor discovery only. Also, based on the LLDP neighbor discovery, port templates can be used on the XMC.

For more information on configuring the following on the XMC server, see the *Extreme Management Center User Guide*.

After you save the configuration, auto-provisioning of the switch begins and the XMC server displays the switch status as **ZTP+ Staged**.

After the auto-provisioning successfully completes, the switch status changes to **ZTP+ Complete**. Also, the switch console displays a log that corresponds to the acknowledgment received from the XMC server on successful auto-provisioning.

14. Verify ZTP+ auto-provisioning on the switch:

View the switch log: `show logging`.

Verify the switch configuration in detail:

- View the consolidated system information (to verify the configured system name, system contact and system location):

```
show system
```

```
show sys-info
```

- View IP configuration:

```
show ip
```

- View VLAN configuration: `show vlan`

- View SNMP users: `show snmp-server user`

- View interface status and configuration: `show interfaces`

- View auto-negotiation advertisement: `show auto-negotiation-capabilities`

- View user roles and log-in permissions:

```
show username
```

- View LLDP neighbor information: `show lldp neighbor`

On the XMC server, verify the status of auto-provisioning by checking the ZTP+ event log.

15. Verify that ZTP+ is disabled on the switch after successful auto-provisioning.

```
show auto-provision
```

### Example

Verify that the switch is enabled for ZTP+ auto-provisioning:

```
Switch:1>show auto-provision
```

```
Admin state      : Enabled
Operational state : Running
```

Connect the switch to the FA Server on the network.

View DNS configuration on the switch.

```
Switch:1>show ip dns
DNS Default Domain name: default.domainname.com
```

```
DNS Servers
-----
198.51.100.2
198.51.100.3
0.0.0.0
```

Enable FA on the switch port that connects to the FA Server. Verify the configuration.

```
Switch:1(config)#fa port-enable 2
Switch:1(config)#show fa port-enable enabled-port
```

```
                Service
Unit Port IfIndex Trunk Advertisement Authentication Keymode
-----
1      2      2              Enabled          Enabled          Strict
```

Configure a management VLAN on the port.

```
Switch:1(config)#fa management i-sid 20200 c-vid 200
```

Verify that the switch receives the management VLAN from the FA Server.

```
Switch:1(config)#show vlan mgmt
Management VLAN: 200

5952GTS-PWR+(config)#show running-config module vlan
...
...
!
! Displaying only parameters different to default
!=====
enable
configure terminal
!
! *** VLAN ***
!
! vlan create 200 type port cist
!
! *** VLAN Phase 2***
!
! vlan mgmt 200
```

Verify that the switch obtains an IP address in the current management VLAN, from the DHCP server.

```
switch:1>show ip
Bootp/DHCP Mode: BootP Or DHCP Or Default IP
```

	Configured	In Use	Last BootP/DHCP
Stack IP Address:	192.168.1.2		0.0.0.0
Switch IP Address:	172.16.120.162	172.16.120.162	0.0.0.0
Switch Subnet Mask:	255.255.255.0	255.255.255.0	0.0.0.0
Mgmt Stack IP Address:	0.0.0.0		
Mgmt Switch IP Address:	0.0.0.0		
Mgmt Subnet Mask:	255.255.255.0		
Mgmt Def Gateway:	1.2.3.4		
Default Gateway:	172.16.120.1	172.16.120.1	0.0.0.0

Verify that the switch connects to and is discovered by the XMC server.

```
Switch:1#show logging
...
...
I 2008-09-17T21:20:09+00:00 5 successfully connected to the XMC server
...
...
```

Update the reference firmware image on the XMC server, which is the firmware version to be pushed to the switch using ZTP+. First upload the firmware image and then set it as the reference image. Also configure the file transfer mode as TFTP or SFTP.

Verify that the switch is updated with the firmware image selected as the reference image on the XMC server:

**\* Note:**

An update is initiated only if the image configured on the switch is different from the reference image on the XMC server.

After the firmware update, the switch reboots and reconnects to the XMC server.

```
Switch:1>show boot
Unit  Agent Image Secondary Image Active Image Diag Image Active Diag
-----
1     7.8.0.021  7.5.0.053      7.8.0.021   7.4.0.8    7.4.0.8
* - Unit requires reboot for new Active Image to be made operational.
# - Unit requires reboot for new Diag to be made operational.
```

View the switch log to view the status of the firmware update:

```
Switch:1#show logging
...
...
I     2008-09-17T21:20:09+00:00    4      successfully connected to the XMC server
I     2008-09-17T21:20:09+00:00    5      the firmware upgrade has started
I     2008-09-17T21:20:09+00:00    5      successfully upgraded the firmware
...
...
```

Verify that the switch reconnects with the XMC server, after the reboot.

```
Switch:1#show logging
...
...
I     2008-09-17T21:20:09+00:00    4      successfully connected to the XMC server
...
...
```

```
Switch:1>show auto-provision
Admin state      : Enabled
Operational state : Running
```

On the XMC server, view the status of the switch. After a successful reconnect, the switch is discovered with a status of **ZTP+ Pending Edit**. At this stage, the switch is ready for ZTP+ auto-provisioning.

As part of device configuration on the XMC server, configure the following to be pushed to the switch. Save the configuration.

- IP configuration
- User configuration
- VLAN configuration
- Port configuration:
- SNMP configuration
- LLDP configuration

After the configuration is saved, auto-provisioning of the switch begins and the XMC server displays the switch status as **ZTP+ Staged**.

After the auto-provisioning successfully completes, the switch status changes to **ZTP+ Complete**. Also, the switch console displays a log that corresponds to the acknowledgment received from the XMC server on successful auto-provisioning.

View ZTP+ auto-provisioning of the switch:

```
Switch:1#show logging
...
...
```

```

I    2008-09-17T21:20:09+00:00    4    successfully connected to the XMC server
I    2008-09-17T21:20:09+00:00    5    the firmware upgrade has started
I    2008-09-17T21:20:09+00:00    5    successfully upgraded the firmware
I    2008-09-17T21:20:09+00:00    4    the auto-provisioning process has started
...
...

```

### Verify ZTP+ auto-provisioning in detail:

- View the consolidated system information (to verify the configured system name, system contact and system location):

```
Switch:1#show system
```

```

System Information:
  Operation Mode:      Switch
  MAC Address:        00-1B-4F-F9-70-00
  PoE Module FW:      1.5.0.11
  Reset Count:        155
  Last Reset Type:    Software Download
  Autotopology:       Enabled
  Base Unit Selection: Non-base unit using rear-panel switch
  sysDescr:           Ethernet Routing Switch 5952GTS-PWR+
                      HW:ROD.7   FW:7.4.0.8   SW:v7.8.0.093
  sysObjectID:        1.3.6.1.4.1.45.3.81.4
  sysUpTime:           9 days, 14:01:04
  sysNtpTime:          NTP not synchronized.
  sysRtcTime:          Tuesday 2020/01/09 16:52:56
  sysServices:         6
  sysContact:
  sysName:             Test switch
  sysLocation:
  Stack sysAssetId:
  Operational license: Base Software
  Installed license:   Base Software

```

```
Switch:1#show sys-info
```

```

Operation Mode:      Switch
Enhanced Secure Mode: Disabled
MAC Address:        00-1B-4F-F9-70-00
PoE Module FW:      1.5.0.11
Reset Count:        155
Last Reset Type:    Software Download
Power Supply 1:     Unavailable
Power Supply 2:     AC-DC-56V1400W-F2B
Power Status :      1- Not Present 2- OK
Autotopology:       Enabled
Pluggable Port 49:  None
Pluggable Port 50:  None
Pluggable Port 51:  None
Pluggable Port 52:  None
Base Unit Selection: Non-base unit using rear-panel switch
sysDescr:           Ethernet Routing Switch 5952GTS-PWR+
                      HW:ROD.7   FW:7.4.0.8   SW:v7.8.0.093
                      Mfg Date:20140712   HW Dev:none
Serial #:            XLIR748P310006
Operational Software: FW:7.4.0.8   SW:v7.8.0.093
Installed software:   FW:7.4.0.8   SW:v7.8.0.093
Operational license:  Base Software
Installed license:    Base Software
sysObjectID:         1.3.6.1.4.1.45.3.81.4
sysUpTime:            9 days, 14:07:52
sysNtpTime:           NTP not synchronized.

```

## Zero Touch Provisioning Plus (ZTP+)

```
sysRtcTime:          Tuesday 2009/06/09 16:59:48
sysServices:         6
sysContact:
sysName:
sysLocation:
Stack sysAssetId:
Unit sysAssetId:
```

- **View IP configuration:**

```
Switch:1#show ip
```

```
Bootp/DHCP Mode: BootP Or DHCP Or Default IP
```

	Configured	In Use	Last BootP/DHCP
Stack IP Address:	198.51.100.2		0.0.0.0
Switch IP Address:	192.0.22.162	192.0.22.162	0.0.0.0
Switch Subnet Mask:	255.255.255.0	255.255.255.0	0.0.0.0
Mgmt Stack IP Address:	0.0.0.0		
Mgmt Switch IP Address:	0.0.0.0		
Mgmt Subnet Mask:	255.255.255.0		
Mgmt Def Gateway:	1.2.3.4		
Default Gateway:	203.0.113.0	203.0.113.0	0.0.0.0

- **View VLAN configuration:**

```
Switch:1#show vlan
```

Id	Name	Type	Protocol	PID	Active	IVL/SVL	Mgmt
1	VLAN #1	Port	None	0x0000	Yes	IVL	Yes
	Port Members: ALL						
100	VLAN #100	Port	None	0x0000	Yes	IVL	No
	Port Members: NONE						

Total VLANs: 2

- **View SNMP user configuration:**

```
Switch:1#show snmp-server user
```

```
User Name: v3-user
SNMP Engine ID: 80:00:02:32:80:02:00:51:58:4C:49:52:37:32:34:54:32:31:30:30:30:38
Authentication Protocol: MD5
Privacy Protocol: AES
Storage Type: Non Volatile(NVRAM)
Status: Active
Views for Unauthenticated Access:
Read View:
Write View:
Notify View:
Views for Authenticated Access:
Read View:
Write View:
Notify View:
Views for Authenticated and Encrypted Access:
Read View:
Write View:
Notify View:
```

- **View interface (port) status and configuration:**

```
Switch:1#show interfaces
```

Port	Trunk	Admin	Oper	Link	LinkTrap	Auto Negotiation	Speed	Duplex	Flow Control
------	-------	-------	------	------	----------	------------------	-------	--------	--------------

```

1          Enable Up   Up   Enabled Enabled          100Mbps Full  Disable
2          Enable Up   Up   Enabled Enabled          1000Mbps Full  Asymm

```

### View auto-negotiation advertisement capabilities for the ports.

```

Switch:1#show auto-negotiation-capabilities

Port Autonegotiation Capabilities
-----
1      10Full 10Half 100Full 100Half 1000Full          AsymmPause
2      10Full 10Half 100Full 100Half 1000Full          AsymmPause
3      10Full 10Half 100Full 100Half 1000Full          AsymmPause

```

- View user roles and log-in permissions:

```

Switch:1#show username

Lockout timeout: 1 min
Lockout retries: 0

Username:          RW
-----
Role name:         RW
Enabled:           Yes
Password aging-time: 0 days
Password expired:  No
Lockout status:    Available
Inactive period:   0 days
SSH access:        Enabled
TELNET access:     Enabled

Username:          RO
-----
Role name:         RO
Enabled:           Yes
Password aging-time: 0 days
Password expired:  No
Lockout status:    Available
Inactive period:   0 days
SSH access:        Enabled
TELNET access:     Enabled

```

- View LLDP neighbor information:

```

Switch:1#show lldp neighbor

-----
LLDP neighbor
-----
Port: 2      Index: 1      Time: 0 days, 00:01:37
      ChassisId: MAC address      00:1c:9c:66:94:00
      PortId:   MAC address      00:1c:9c:66:94:04
-----
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 1

```

### Verify that ZTP+ is disabled on the switch, after successful auto-provisioning.

```

Switch:1>show auto-provision

Admin state      : Disabled
Operational state : Completed

```

# Glossary

<b>Address Resolution Protocol (ARP)</b>	Maps an IP address to a physical machine address, for example, maps an IP address to an Ethernet media access control (MAC) address.
<b>Agent Auto Unit Replacement (AAUR)</b>	Enabled by default, AAUR inspects all units in a stack and downloads the stack software image to any joining unit with a dissimilar image.
<b>American Standard Code for Information Interchange (ASCII)</b>	A code to represent characters in computers. ASCII uses uppercase and lowercase alphabetic letters, numeric digits, and special symbols.
<b>Authentication, Authorization, and Accounting (AAA)</b>	Authentication, Authorization, and Accounting (AAA) is a framework used to control access to a network, limit network services to certain users, and track what users do. Authentication determines who a user is before allowing the user to access the network and network services. Authorization allows you to determine what you allow a user to do. Accounting records what a user is doing or has done.
<b>Auto MDIX</b>	The automatic detection of transmit and received twisted pairs. When Auto MDIX is active, you can use any straight or crossover category 5 cable to provide connection to a port. You must enable Autonegotiation to activate Auto MDIX.
<b>Auto polarity</b>	Compensates for reversal of positive and negative signals on the receive cables. When you enable autonegotiation, auto polarity can reverse the polarity of a pair of pins to correct polarity of received data.
<b>Auto Unit Replacement (AUR)</b>	Allows users to replace a unit from a stack while retaining the configuration of the unit. Stack power must remain on during the unit replacement. AUR does not work in a stack of two units only.
<b>Auto-Detection and Auto-Configuration (ADAC)</b>	Provides automatic switch configuration for IP phone traffic support and prioritization. ADAC can configure the switch whether it is directly connected to the Call Server or uses a network uplink.
<b>Automatic PVID</b>	Automatically sets the port-based VLAN ID when you add the port to the VLAN. The PVID value is the same value as the last port-based VLAN ID associated with the port.



<b>Autonegotiation</b>	Allows the switch to select the best speed and duplex modes for communication between two IEEE-capable devices.
<b>Autosensing</b>	Determines the speed of the attached device if it is incapable of autonegotiation or if it uses an incompatible form of autonegotiation.
<b>Autotopology</b>	An Enterprise Network Management System (ENMS) protocol that automates and simplifies discovery and collection of network topology information, presented in a table.
<b>base unit (BU)</b>	When you connect multiple switches into a stack, one unit, and only one unit, must be designated as a base unit to perform stack configuration tasks. The position of the unit select switch, on the back of the switch, determines base unit designation.
<b>Bootstrap Protocol (BootP)</b>	A User Datagram Protocol (UDP)/Internet Protocol (IP)-based protocol that a booting host uses to configure itself dynamically and without user supervision.
<b>Bridge Protocol Data Unit (BPDU)</b>	A data frame used to exchange information among the bridges in local or wide area networks for network topology maintenance.
<b>Bridging</b>	A forwarding process, used on Local Area Networks (LAN) and confined to network bridges, that works on Layer 2 and depends on the Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP). Bridging is also known as MAC forwarding.
<b>CLI</b>	Command Line Interface (CLI) is a text-based, common command line interface used for device configuration and management across Extreme Networks products.
<b>CLI modes</b>	Differing command modes are available within the text-based interface, dependant on the level of user permissions determined by logon password. Each successive mode level provides access to more complex command sets, from the most restrictive—show level only, to the highest configuration levels for routing parameters, interface configuration, and security.
<b>Custom AutoNegotiation Advertisement (CANA)</b>	Custom AutoNegotiation Advertisement offers improved control over the autonegotiation process. The system advertises all port capabilities that include 10 Mb/s, 100 Mb/s, 1000 Mb/s, 2500 Mb/s, 10000 Mb/s speeds, and duplex and half-duplex modes of operation. This advertisement results in autonegotiation between the local and remote end that settles on the highest common denominator. Custom AutoNegotiation Advertisement can advertise a user-defined subset of the capabilities that settle on a lower or particular capability.
<b>Custom AutoNegotiation</b>	Custom AutoNegotiation Advertisement offers improved control over the autonegotiation process. The system advertises all port capabilities that include 10 Mb/s, 100 Mb/s, 1000 Mb/s, 2500 Mb/s, 10000 Mb/s speeds,

<b>Advertisement (CANA)</b>	and duplex and half-duplex modes of operation. This advertisement results in autonegotiation between the local and remote end that settles on the highest common denominator. Custom AutoNegotiation Advertisement can advertise a user-defined subset of the capabilities that settle on a lower or particular capability.
<b>daemon</b>	A program that services network requests for authentication and authorization. A daemon verifies, identifies, grants or denies authorizations, and logs accounting records.
<b>Differentiated Services (DiffServ)</b>	A network architecture enabling service providers and enterprise network environments to offer varied levels of service for different traffic types.
<b>Differentiated Services Code Point (DSCP)</b>	The first six bits of the DS field. The DSCP uses packet marking to guarantee a fixed percentage of total bandwidth to each of several applications (guarantees quality of service).
<b>Differentiated Services Quality of Service (DiffServ QoS)</b>	Allows specific level of performance designation, on a packet-by-packet basis, for high performance and reliable service for voice or video over IP, or for preferential treatment of data over other traffic.
<b>Domain Name System (DNS)</b>	A system that maps and converts domain and host names to IP addresses.
<b>Duplicate Address Detection (DAD)</b>	A method used to discover duplicate addresses in an IPv6 network.
<b>Dynamic Host Configuration Protocol (DHCP)</b>	A standard Internet protocol that dynamically configures hosts on an Internet Protocol (IP) network for either IPv4 or IPv6. DHCP extends the Bootstrap Protocol (BOOTP).
<b>equal cost multipath (ECMP)</b>	Distributes routing traffic among multiple equal-cost routes.
<b>Extensible Authentication Protocol over LAN (EAPoL)</b>	A port-based network access control protocol. EAPoL provides security in that it prevents users from accessing network resources before they are authenticated.
<b>flash memory</b>	All switch configuration parameters are stored in flash memory. If you store switch software images in flash memory, you can update switch software images without changing switch hardware.
<b>Gigabit Ethernet (GbE)</b>	Ethernet technology with speeds up to 100 Gbps.

<b>Gigabit Interface Converter (GBIC)</b>	A hotswappable input and output enhancement component, designed for use with Extreme Networks products, that allows Gigabit Ethernet ports to link with other Gigabit Ethernet ports over various media types.
<b>Internet Control Message Protocol (ICMP)</b>	A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.
<b>Internet Group Management Protocol (IGMP)</b>	IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.
<b>Internet Protocol Flow Information eXport (IPFIX)</b>	An IETF standard that improves the Netflow V9 protocol. IPFIX monitors IP flows.
<b>Internet Protocol Manager (IP Manager)</b>	Used to limit access to switch management features by defining IP addresses allowed access to the switch.
<b>Internet Protocol Security (IPsec)</b>	Internet Protocol security (IPsec) is a set of security protocols and cryptographic algorithms that protect communication in a network. Use IPsec in scenarios where you need to encrypt packets between two hosts, two routers, or a router and a host.
<b>Internet Protocol version 4 (IPv4)</b>	The protocol used to format packets for the Internet and many enterprise networks. IPv4 provides packet routing and reassembly.
<b>Internet Protocol version 6 (IPv6)</b>	An improved version of the IP protocol, IPv6 improves the IPv4 limitations of security and user address numbers.
<b>Layer 2</b>	Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.
<b>Layer 3</b>	Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).
<b>light emitting diode (LED)</b>	A semiconductor diode that emits light when a current passes through it.
<b>Link Aggregation</b>	Provides the mechanism to create and manage trunk groups automatically using Link Aggregation Control Protocol (LACP).
<b>Link Aggregation Control Protocol (LACP)</b>	A network handshaking protocol that provides a means to aggregate multiple links between appropriately configured devices.
<b>Link Layer Discovery Protocol (LLDP)</b>	Link Layer Discovery Protocol is used by network devices to advertise their identities. Devices send LLDP information at fixed intervals in the form of

	Ethernet frames, with each frame having one Link Layer Discovery Protocol Data Unit.
<b>Local Area Network (LAN)</b>	A data communications system that lies within a limited spatial area, uses a specific user group and topology, and can connect to a public switched telecommunications network (but is not one).
<b>management information base (MIB)</b>	The MIB defines system operations and parameters used for the Simple Network Management Protocol (SNMP).
<b>mask</b>	A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.
<b>maximum transmission unit (MTU)</b>	The largest number of bytes in a packet—the maximum transmission unit of the port.
<b>media</b>	A substance that transmits data between ports; usually fiber optic cables or category 5 unshielded twisted pair (UTP) copper wires.
<b>Media Access Control (MAC)</b>	Arbitrates access to and from a shared medium.
<b>media access unit (MAU)</b>	The equipment in a communications system that adapts or formats signals, such as optical signals, for transmission over the propagation medium.
<b>Message Digest 5 (MD5)</b>	A one-way hash function that creates a message digest for digital signatures.
<b>MultiLink Trunking (MLT)</b>	A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.
<b>Multiple Spanning Tree Protocol (MSTP)</b>	Configures multiple instances of the Rapid Spanning Tree Protocol (RSTP) on the switch.
<b>Network Time Protocol (NTP)</b>	A protocol that works with TCP that assures accurate local time keeping with reference to radio and atomic clocks located on the Internet. NTP synchronizes distributed clocks within milliseconds over long time periods.
<b>nonbase unit (NBU)</b>	A nonbase unit is any unit in a stack except the base unit.
<b>NonVolatile Random Access Memory (NVRAM)</b>	Random Access Memory that retains its contents after electrical power turns off.

<b>Open Shortest Path First (OSPF)</b>	A link-state routing protocol used as an Interior Gateway Protocol (IGP).
<b>Policy-Enabled Networking</b>	User-defined characteristics that can be set in policies used to control and monitor traffic.
<b>port</b>	A physical interface that transmits and receives data.
<b>port mirroring</b>	A feature that sends received or transmitted traffic to a second destination.
<b>port VLAN ID</b>	Used to coordinate VLANs across multiple switches. When you create a port-based VLAN on a switch, assign a VLAN identification number (VLAN ID) and specify the ports that belong to the VLAN.
<b>Power over Ethernet (PoE)</b>	The capacity of a switch to power network devices, according to the 802.3af standard, over an Ethernet cable. Devices include IP phones, Wireless LAN Access Points (WLAN AP), security cameras, and access control points.
<b>prefix</b>	A group of contiguous bits, from 0 to 32 bits in length, that defines a set of addresses.
<b>Protocol Data Units (PDUs)</b>	A unit of data that is specified in a protocol of a specific layer and that consists of protocol-control information of the specific layer and possibly user data of that layer.
<b>Proxy Address Resolution Protocol (Proxy ARP)</b>	Allows the switch to respond to an Address Resolution Protocol (ARP) request from a locally attached host (or end station) for a remote destination.
<b>quality of service (QoS)</b>	QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.
<b>Rapid Spanning Tree Protocol (RSTP)</b>	Reduces the recovery time after a network breakdown. RSTP enhances switch-generated Topology Change Notification (TCN) packets to reduce network flooding.
<b>Rate Limiting</b>	Rate limiting sets the percentage of traffic that is multicast, broadcast, or both, on specified ports.
<b>real time clock</b>	Provides the switch with time information if Simple Network Time Protocol (SNTP) time is unavailable.
<b>redundant power supply unit (RPSU)</b>	Provides alternate backup power over a DC cable connection into an Extreme Networks Ethernet Routing Switch.

<b>Remote Authentication Dial-in User Service (RADIUS)</b>	A protocol that authenticates, authorizes, and accounts for remote access connections that use dial-up networking and Virtual Private Network (VPN) functionality.
<b>request for comments (RFC)</b>	A document series published by the Internet Engineering Task Force (IETF) that describe Internet standards.
<b>routing switch</b>	Virtualizes the physical router interfaces to switches. A virtual router port, or interface, acts as a router port to consolidate switching and routing functions in the broadcast domain, or between broadcast domains, and enable IP routing for higher traffic volumes.
<b>Secure Shell (SSH)</b>	SSH uses encryption to provide security for remote logons and data transfer over the Internet.
<b>SFP</b>	A hot pluggable, small form-factor pluggable (SFP) transceiver, which is used in Ethernet applications up to 1 Gbps.
<b>shortest path first (SPF)</b>	A class of routing protocols that use Dijkstra's algorithm to compute the shortest path through a network, according to specified metrics, for efficient transmission of packet data.
<b>Simple Network Time Protocol (SNTP)</b>	Provides a simple mechanism for time synchronization of the switch to any RFC 2030-compliant Network Time Protocol (NTP) or SNTP server.
<b>spanning tree</b>	A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.
<b>Spanning Tree Group (STG)</b>	A collection of ports in one spanning-tree instance.
<b>Spanning Tree Protocol (STP)</b>	MAC bridges use the STP to exchange information across Local Area Networks to compute the active topology of a bridged Local Area Network in accordance with the Spanning Tree Protocol algorithm.
<b>stack</b>	Stackable Extreme Networks Ethernet Routing Switch can be connected in a stack configuration of two or more units, up to eight units maximum. A switch stack operates and is managed as a single virtual switch.
<b>stack IP address</b>	An IP address must be assigned to a stack so that all units can operate as a single entity.
<b>stack unit</b>	Any switch within a stack.

<b>stand-alone</b>	Refers to a single Extreme Networks Ethernet Routing Switch operating outside a stack.
<b>Terminal Access Controller Access Control System plus (TACACS+)</b>	Terminal Access Controller Access Control System plus (TACACS+) is a security protocol that provides centralized validation of users who attempt to gain access to a router or network access server. TACACS+ uses Transmission Control Protocol (TCP) for its transport to ensure reliable delivery and encrypts the entire body of the packet. TACACS+ provides separate authentication, authorization, and accounting services. TACACS+ is not compatible with previous versions of TACACS.
<b>Time Domain Reflectometer (TDR)</b>	Provides diagnostic capability on Ethernet copper ports to test connected cables for defects. The TDR interrupts 10/100 MB/s links but does not affect 1 GB/s links.
<b>time-to-live (TTL)</b>	The field in a packet used to determine the valid duration for the packet. The TTL determines the packet lifetime. The system discards a packet with a TTL of zero.
<b>Transmission Control Protocol (TCP)</b>	Provides flow control and sequencing for transmitted data over an end-to-end connection.
<b>Trivial File Transfer Protocol (TFTP)</b>	A protocol that governs transferring files between nodes without protection against packet loss.
<b>trunk</b>	A logical group of ports that behaves like a single large port.
<b>Type of Service (TOS)</b>	A field in the IPv4 header that determines the Class of Service prior to the standardization of Differentiated Services.
<b>unit select switch</b>	Use the unit select switch on the back of a unit in the stack to designate the unit as the base or nonbase unit.
<b>unshielded twisted pair (UTP)</b>	A cable with one or more pairs of twisted insulated copper conductors bound in a single plastic sheath.
<b>User Datagram Protocol (UDP)</b>	In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.
<b>Virtual Local Area Network (VLAN)</b>	A Virtual Local Area Network is a group of hosts that communicate as if they are attached to the same broadcast domain regardless of their physical location. VLANs are layer 2 constructs.
<b>Virtual Router Redundancy Protocol (VRRP)</b>	A protocol used in static routing configurations, typically at the edge of the network. This protocol operates on multiple routers on an IP subnet and elects a primary gateway router. When the primary router fails, a backup router is quickly available to take its place.

**Voice over IP (VOIP)**

The technology that delivers voice information in digital form in discrete packets using the Internet Protocol (IP) rather than the traditional circuit-committed protocols of the public switched telephone network (PSTN).

**XFP**

A pluggable 10 gigabit transceiver capable of providing different optical media for a switch. The XFP is similar to an SFP transceiver but is larger in size.