ExtremeSwitching

Configuring Systems on Ethernet Routing Switch 3600 Series

Release 6.4
9036478-00 Rev AB
March 2020

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, please see: 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: www.extremenetworks.com/support/policies/software-licensing

Contents

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 the information and procedures required to configure the switch software.

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...
Important:	A situation that can cause serious inconvenience.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Danger:	Situations that will result in severe bodily injury; up to and including death.
Warning:	Risk of severe personal injury or critical loss of data.
Caution:	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) 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. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	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.

Table continues…

Convention	Description
	Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** 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 `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware/software compatibility matrices for Campus and Edge products
Supported transceivers and cables for Data Center products
Other resources, like 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/.

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

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.
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.

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 sections detail 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 261
- Configuring ZTP+ using the CLI on page 264
- Configuring ZTP+ Examples on page 269

Chapter 3: System configuration

Use the information in this chapter to help you understand System configuration, and how to configure the System using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

This chapter includes the following sections:

- System configuration fundamentals
- System configuration using CLI
- Configuring the switch using EDM

System configuration fundamentals

ERS 3600 Series switch models

The following table lists the different ERS 3600 Series models and the key features.

ERS 3600 Series model	Key features	Part number
ERS 3626GTS	• 24 10/100/1000 ports • Two shared SFP ports • Two 1/10 Gigabit SFP+ ports operating in dual mode as uplink ports • Two 10 Gigabit SFP+ ports as either uplink or stacking ports • Non-PoE • Stackable	AL3600?05-E6
ERS 3626GTS-PWR+	• 24 10/100/1000 802.3at PoE ports • Two shared SFP ports • Two 1/10 Gigabit SFP+ ports operating in dual mode as uplink ports	AL3600?15-E6

Table continues…

ERS 3600 Series model	Key features	Part number
	• Two 10 Gigabit SFP+ ports as either uplink or stacking ports • Stackable	
ERS 3650GTS	• 48 10/100/1000 ports • Two shared SFP ports • Two 1/10 Gigabit SFP+ ports operating in dual mode as uplink ports • Two 10 Gigabit SFP+ ports as either uplink or stacking ports • Non-PoE • Stackable	AL3600A06-E6
ERS 3650GTS-PWR+	• 48 10/100/1000 802.3at PoE ports and 2 shared SFP ports • Two 1/10 Gigabit SFP+ ports operating in dual mode as uplink ports • Two 10 Gigabit SFP+ ports as either uplink or stacking ports • Stackable	AL3600A16-E6

Stack Capabilities

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

- stand-alone

  Additional uplinks or connections to servers or power users are provided. Regular port configuration parameters, such as Spanning Tree, EAP, VLAN Tagging, MLT/DMLT/VLACP, and port enable/disable are supported.

  Fixed port speed is provided at 1000 Mbps Full Duplex operation with the insertion of a supported SFPs.

- stack

  Important:

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

  The switches have a built-in cascade port to stack up to eight units. The total stacking bandwidth in a stack is 80 Gbps with 20 Gbps in each direction.

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

  To set up a stack, perform the following procedure:

  1. Power down all switches.

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

For more information about configuring stacking, see Installing Ethernet Routing Switch 3600 Series.

Stack Considerations for ERS 3600 Models

SFP+ trunk design

It is recommended that you alternate MLT or LAG members to every other switch in the stack when using 10G interfaces. This allows a shorter path to be taken across the stacking backplane by access port traffic that more frequently sends data across a trunk link rather than to another access port. Additionally, this configuration supports the need for communication between hosts connected to access ports and is within the performance requirements of the full duplex access port bandwidth, satisfying common host-to-host communication needs.

Consideration must also be given to the aggregate bandwidth requirements of the access ports that are at, or over, stack capacity. You can use additional SFP+ interfaces in additional groups as required, such as for fault tolerance when connecting to a network core. However, you must keep this relative to the overall available bandwidth of the stack.

SFP trunk/uplink design

You can use fiber trunks to create connections to network servers or create MLTs and LAGs when resilient trunks to a network core are required. As the bandwidth of these SFP interfaces is typically less than 1Gbps, few considerations are required for these types of MLTs. However, Extreme Networks recommends that you alternate these trunk interfaces equally across the stack. There is less of a need to limit the number of these trunks as the primary constraint is the number LAG groups supported by the switch.

Trunks and Access Port Utilization

You must consider the aggregation of all trunk and access port traffic such that the entire design delivers the proper amount of total bandwidth to the entire network.

Access Port Utilization

Although access ports are typically connected using a Gigabit Ethernet access port, the average peak unitization of that port is typically less than 1Gbps. Therefore, large stack designs must consider the peak utilization of connected users requiring IP data, voice, and video services during peak hours.

Network designs can support up to 384 access ports on stack-enabled switches. This allows for half of the 80Gbps stacking bandwidth to be utilized for access ports, while leaving the greater of 40Gbps available for servicing those access ports using the switch trunks or uplinks.

Trunk/Uplink Port Utilization

The switch provides MLT and LAG options so that redundant links can use separate hardware platforms in a stack to provide the highest level of resiliency. These types of connections can aggregate the available bandwidth over the trunk or uplink.

You must consider the aggregate bandwidth of these trunks and uplinks to ensure they do not exceed the capacity of the stacked bandwidth. Therefore, you must consider not only the trunk or uplink peak utilization requirements, but also the access port aggregate utilization.

In configurations where voice and data services are to be delivered on the access ports to a large numbers of users, you must allocate sufficient bandwidth to the trunk and uplink ports to support the access port traffic. In these situations, Extreme Networks recommends that you limit the aggregate of MLT and LAG port utilization to 40Gbps. This amount represents any combination of SFP, and or SFP+ interfaces while also adhering to the MLT and LAG scaling limitations.

You can configure QoS on the switch to manage traffic during periods of over-subscription during peak hours.

Considerations for 8 unit stacks

Design element	Design consideration
Uplink, MLT, LAGs, SFP+ interfaces	Every other switch in stack
Stacking capacity – 8 switches	80Gbps
Uplink aggregate[1] - 8 switches	40Gbps – 4 SFP+
Access port aggregate[1] - 8 switches	40Gbps

Note:

[1] Designs might vary and aggregate throughput might vary depending on access or trunk port utilization required by the design. These are recommendations based on the use case defined above for a typical UC-enabled office.

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
```

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

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

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

CFG mirror image process

The CFG mirror image process is triggered by specific events.

Power Cycle:

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

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

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

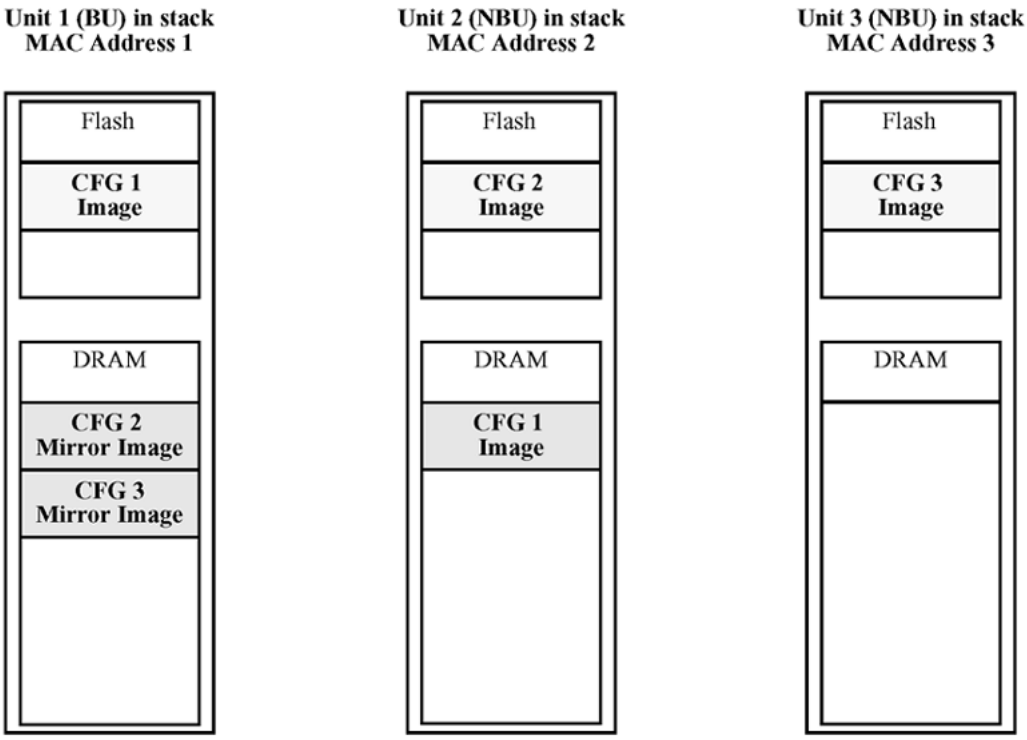


Figure 1: CFG mirror process in stack

Adding a unit:

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

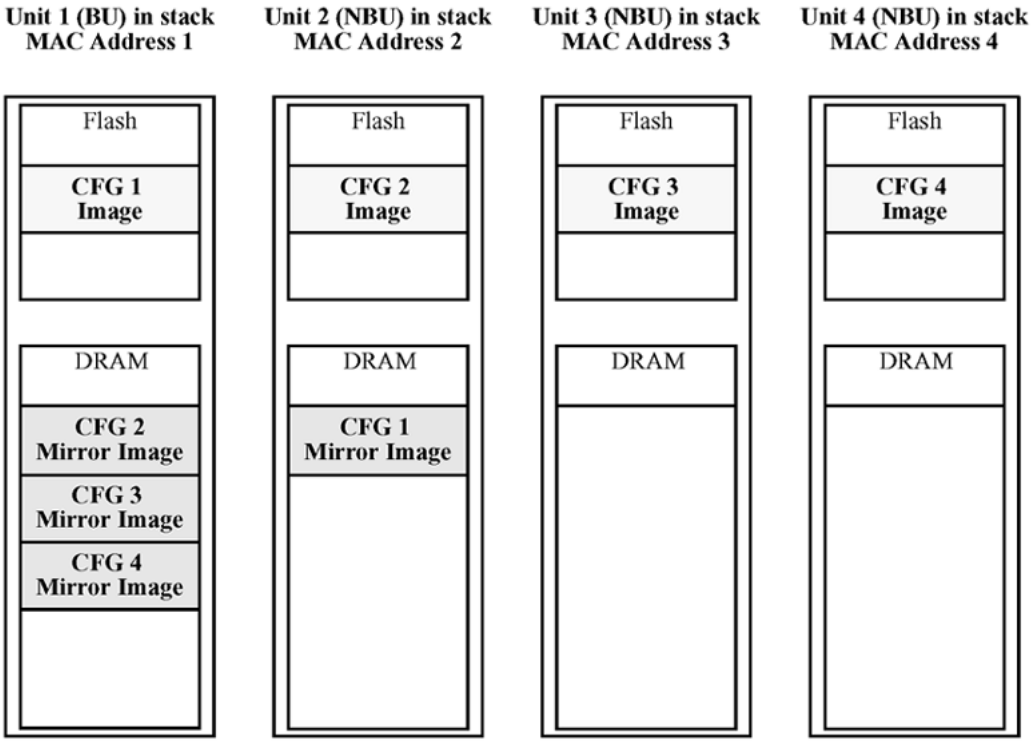


Figure 2: CFG mirror images in the stack after adding unit 4

Removing an NBU:

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

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

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

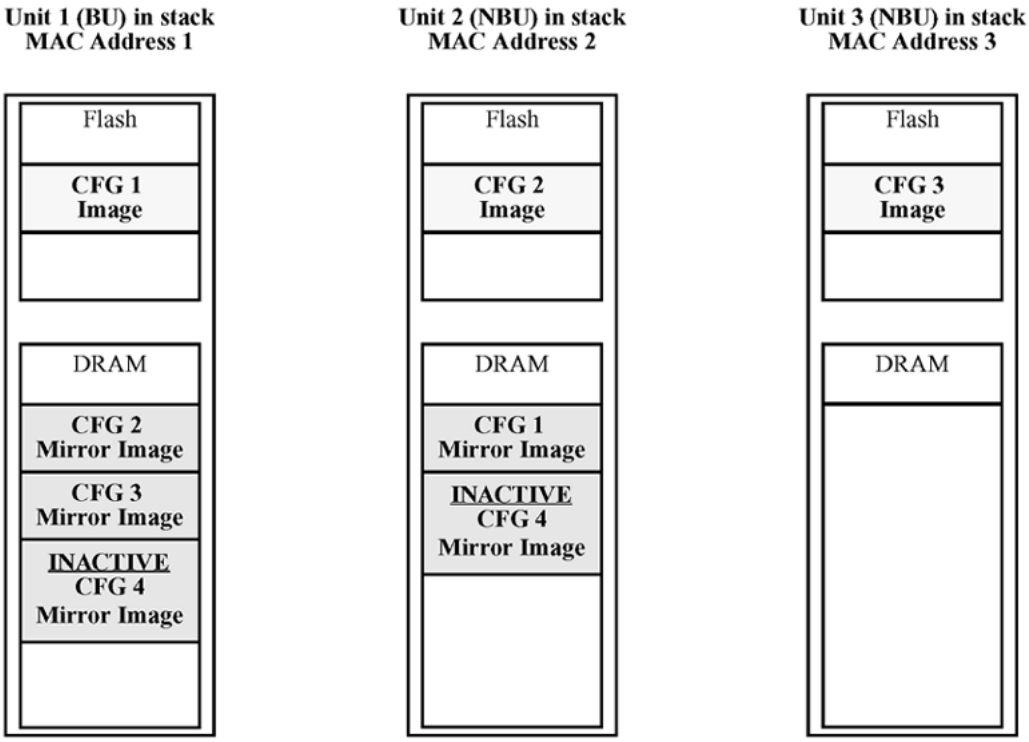


Figure 3: CFG mirror images after removing unit 4

Removing a BU:

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

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

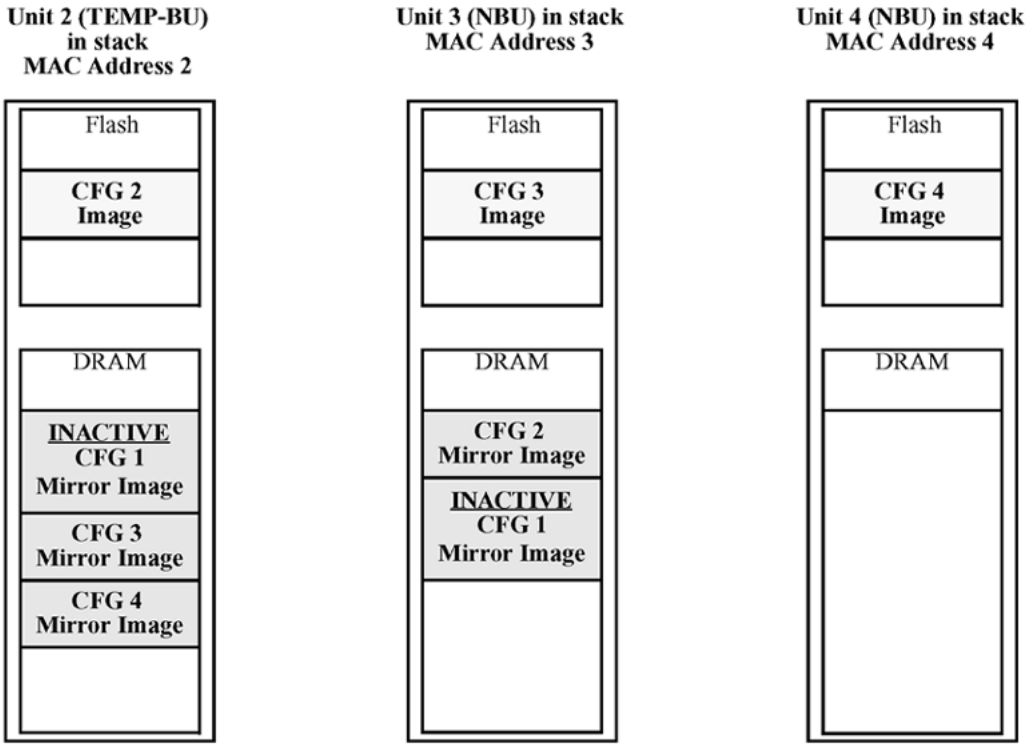


Figure 4: CFG mirror images in the stack after removing the BU (unit 1)

As shown in the previous figure:

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

Note:

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

Restoring a CFG image

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

Important:

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

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

The image restore process consists of the following steps:

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

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

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

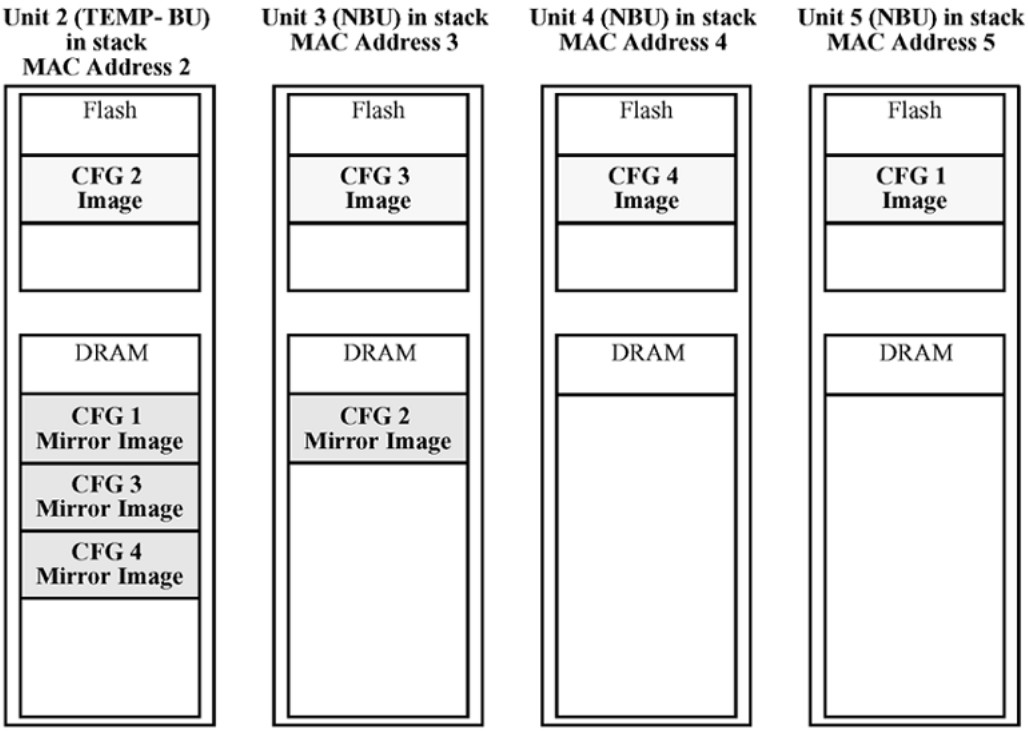


Figure 5: CFG mirror images in the stack after adding unit 5

Synchronizing the CFG mirror images with CFG images

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

Agent Auto Unit Replacement

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

Agent Auto Unit Replacement functions in the following manner:

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

AUR and AAUR Operations for BU Replacement in 2 High Stack

To ensure the AUR and AAUR features operate successfully during the BU replacement in a 2-high stack, follow these guidelines:

1. Before a unit is replaced, enter the command `show stack auto-unit-replacement` to find out if that unit is ready for replacement.
2. Remove the BU from the stack. The remaining unit (NBU) becomes stand-alone.
3. Before the new BU is connected to the NBU, power-cycle the new BU to ensure that it does not have a valid AUR Data Record in the memory.

Stack Forced Mode

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

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

You can configure Stack Forced Mode through CLI. Refer to Enabling or disabling stack forced mode on page 70.

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

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

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

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

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

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

IPv6 management fundamentals

This section provides information about the IPv6 management feature.

The IPv6 header

The IPv6 header contains the following fields:

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

IPv6 addresses

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

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

The switch does not support stateless or stateful address configuration. The device does not try to obtain ipv6 parameters from a router and it does not query an IPv6 DHCP server, if it does not have an IPv6 address configured. The IPv6 global address must be entered manually. The link-local IPv6 address is generated automatically, based on the MAC address of the device when the IPv6 interface is attached to the management VLAN.

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:nn 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 six contiguous fields containing zeroes with a double colon (::):FF01::43

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

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

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

or

::13.1.68.3

IPv6 extension headers

IPv6 extension headers describe processing options. Each extension header contains a separate category of options. A packet can include zero or more extension headers.

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 can fit 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 3: IPv4 and IPv6 differences

Feature	IPv4	IPv6
Address length	32 bits	128 bits
IPsec support (See Note 1)	Optional	Required
QoS support	Limited	Improved
Fragmentation	Hosts and routers	Hosts only
Minimum MTU (packet size)	576 bytes	1280 bytes
Checksum in header	Yes	No
Options in header	Yes	No
Link-layer address resolution	ARP (broadcast)	Multicast Neighbor Discovery Messages
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router discovery (See Note 2)	Optional	Required
Uses broadcasts	Yes	No
Configuration (See Note 3)	Manual, DHCP	Manual
Note 1: IPsec is not supported. Note 2: The switch does not perform Router discovery or advertise as a router. Note 3: The switch does not implement any form of automatic configuration of IPv6 address.		

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 nexthop 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

ND messages

The following table shows new ICMPv6 message types.

Table 4: IPv4 and IPv6 neighbor discovery comparison

IPv4 neighbor function	IPv6 neighbor function	Value
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-

Table continues…

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

Neighbor discovery cache

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

The neighbor discovery cache can contain the following types of neighbors

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

The following table describes neighbor cache states.

Table 5: Neighbor cache states

State	Value
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 multilink 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. The switch does not support stateless automatic configuration; therefore, no router solicitation messages are sent by the switch.

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 host mode enhancement

IPv6 host mode enhancement is an extension of IPv6 management application, which supports several settings that are not available by default on the in-band/out-of-band management interface. Host Enhancement in the IPv6 stack is compiled in the following two ways:

- HOST mode (for management only releases): When compiled in HOST mode, host enhancement features are available on the management interface.
- ROUTER mode (for routing releases): When compiled in ROUTER mode, host enhancement features are available on the out-of-band interface.

The feature allows the user to perform the following tasks:

- Start/stop Stateless Address Auto-Configuration (SLAAC).
- Configure interface to honor **Redirect** messages.
- Display or clear the **ipv6 destination cache**.
- Display **Default Router List** and the active router.
- View the remaining preferred or valid life for auto-configured addresses.
- View the MLD host cache.
- Configure the device to not respond to Echo Requests destined to multicast addresses.
- Configure ICMP error quota for the error messages generated by the device.
- Configure global IPV6 address from a given prefix and Extended Unique Identifier (EUI).

- Configure two neighbor discovery parameters:
  - number of packets sent during duplicate address detection
  - hop limit value for the interface

Limitations

The following are the limitations for IPv6 host mode enhancements:

- In the Host Mode, only one IPV6 interface is supported and it will be associated to the management VLAN.
- Maximum 16 prefixes can be learned through Router Advertisement.
- Maximum four routers are kept in default routers list.
- MIB support for the new Host Mode structures is not implemented.
- Only one Global IPV6 address can be configured (manual) by the user.
- For routing platforms, host enhancement features work on Out of band (OOB) Management interface only when IPv6 forwarding is disabled.

IPv6 loopback

IPv6 Loopback provides support for loopback IPv6 interface on a switch/stack. With IPv6 loopback functionality, you can check if IPv6 protocol is working properly prior to connecting to other devices. When an IPv6 loopback interface is configured, a circuit is created with a loopback address. No link-local address is added to the circuit. IPv6 packets are sent on this circuit up to Layer 2 point, and then these packets are looped back. A maximum number of four loopback interfaces out of 16 can be created on a switch/stack.

IPv6 Loopback complies with RFC 3484, Default Address Selection for Internet Protocol version 6 (IPv6).

Note:

You must enable IPv6 globally, before you configure a loopback IPv6 interface.

Limitations

The following are the limitations for IPv6 Loopback interface:

- Only one IPv6 address can be assigned to one IPv6 loopback interface.
- Only four IPv6 loopback interfaces can exist on a switch/stack.
- The CLI commands are available in stack only on the Base Unit (BU).

.

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 3600 Series.

Show FLASH History

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

- Diagnostics Image
- Agent Image
- Configuration Area
- Auxiliary Configuration Area
- CRC Block

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.

For more information about policy-enabled networking, see Configuring Quality of Service on Ethernet Routing Switch 3600 Series .

Power over Ethernet

ERS 3626GTS-PWR+ and ERS 3650GTS-PWR+ provide IEEE 802.3at-compliant power or PoE+ on all 10/100/1000 RJ-45 ports.

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

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

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

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.

Low PoE power setting

Important:

Low PoE power setting is supported on the ERS3626GTS-PWR+ only.

The switch can be configured to low PoE power mode. In this mode, the fan speed is reduced to accommodate silent operation for open environments where reduced noise from the fans is required. The surrounding ambient air temperature for use of this feature is required to be 30 degrees Celsius (86 F) or lower. The available PoE budget for the switch when operating in low-power-budget is limited to 90 Watts in total (802.3af/at) allowing the switch to operate with an acoustic output of 40 db or less. This feature is supported in stand-alone mode only.

For more information, see the following:

- Configuring PoE power mode using CLI on page 89
- Configuring PoE power mode using EDM on page 143

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.

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 can specify port-based monitoring for ingress and/or egress to a specific port. You can also attach a probe device or equivalent, to the designated monitor port. When a port is operating as a monitor port, forwarding is not allowed on that port.

For more information about port mirroring, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

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.

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.

The hardware restrictions on this platform do not allow you to determine if the traffic from a port is the cause of excess broadcast or multicast traffic. Consequently you cannot perform port specific actions, such as disabling a port. You can generate a trap to detect the excess traffic or you can configure the switch to store a message in the system log when the traffic on the port exceeds the threshold value. This message in the system log conveys that some traffic to the switch is dropped.

When the volume of either packet type is high, placing severe strain on the network (often referred to as a storm), you can set the forwarding rate of those packet types to not exceed a specified percentage of the total available bandwidth. The pps (Packets Per Second) value you set is a small amount of the maximum value of pps for the maximum available bandwidth that is 262143 pps.

For more information about rate limiting, see Configuring Security on Ethernet Routing Switch 3600 Series.

Manual-MDI/X

A Medium Dependent Interface (MDI) describes the interface (both physical and electrical) in a computer network from a physical layer implementation to the physical medium used to carry the transmission. Ethernet over twisted pair also defines a medium dependent interface crossover (MDIX) interface. Auto MDI-X ports on newer network interfaces detect if the connection would require a crossover, and automatically chooses the MDI or MDI/X configuration to properly match the other end of the link.

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.

Autosense and Autonegotiate

The switch is an autosensing and autonegotiating device.

- The term autosense refers to the ability of a port to sense the speed of an attached device.

- The term autonegotiation refers to a standardized protocol (IEEE 802.3u) that exists between two IEEE 802.3u-capable devices. Autonegotiation lets the switch select the best of speed and duplex modes.

Autosensing is used when the attached device is not capable of autonegotiation or is using a form of autonegotiation that is not compatible with the IEEE 802.3u standard. In this case, because it is not possible to sense the duplex mode of the attached device, the switch reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the switch, the ports negotiate down from 1000 Mb/s speed and full-duplex mode and from 100 Mb/s speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

Advertising Custom Autonegotiation

Custom Autonegotiation Advertisements (CANA) lets you customize the capabilities that you advertise. For example, if a port is not capable of 10/100/1000 full duplex operation, the port can be configured to only advertise 10 half-duplex capabilities.

CANA lets you control the capabilities that are advertised by the Ethernet switches as part of the autonegotiation process. In the current software releases, autonegotiation can either be enabled or disabled.

When autonegotiation is disabled, the hardware is configured for a single (fixed) speed and duplex value. When autonegotiation is enabled, the advertisement made by the product is a constant value based upon all speed and duplex modes supported by the hardware.

When autonegotiating, the switch selects the highest common operating mode supported between the switch and its link partner.

In certain situations, it is useful to autonegotiate a specific speed and duplex value. In these situations, the switch can allow for attachment at an operating mode other than its highest supported value.

For example, if the switch advertises only a 100 Mbps full-duplex capability on a specific link, the link goes active only if the neighboring device is also capable of autonegotiating a 100 Mbps full-duplex capability. This prevents mismatched speed and duplex modes if customers disable autonegotiation on the neighboring device.

Important:

The CANA feature is available for 10/100 Ethernet ports of ERS 3626GTS switches (not available for rear ports).

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.

For more information, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

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.

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
- 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

BootP, DHCP or Default IP

The switch operates in the BootP, DHCP or Default IP (the default mode) as follow:

- After the switch is reset or power cycled, if the switch has a configured IP address other than 0.0.0.0 or the default IP address, then the switch uses the configured IP address.
- If the configured IP address is 0.0.0.0 or the default IP address (192.168.1.1/24), then the switch attempts BootP for 1 minute.
- If BootP succeeds, then the switch uses the IP information provided.
- If BootP fails, 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.
- When a stack is booted, the default IP address is 192.168.1.2 instead of 192.186.1.1 when in standalone.

BootP Always

This option lets you manage the switch that is configured with the IP address obtained from the BootP server. The switch operates in the BootP Always mode as follows:

- The switch continues to broadcast BootP requests, regardless of whether an in-band IP address is set from the console terminal.
- If the switch receives a BootP reply that contains an in-band IP address, the switch uses this new in-band IP address.
- If the BootP server is not reachable, you cannot change the in-band IP address until the BootP mode is set to BootP Disabled. However, after a period of a few minutes (approximately 10 minutes), the switch automatically enters the BootP Disabled mode. You can then configure the IP address with CLI.

If an IP address is not currently in use, these actions take effect immediately. If an IP address is currently in use, these actions take effect only after the switch is reset or power cycled.

BootP Disabled

This option lets you manage the switch by using the IP address set from the console terminal. The switch operates in the BootP Disabled mode as described in the following steps:

- The switch does not broadcast BootP requests, regardless of whether an IP address is set from the console terminal.
- The switch can be managed only by using the in-band switch IP address set from the console terminal.

BootP or Last Address

This option lets you manage the switch even if a BootP server is not reachable. The switch operates in the BootP or Last Address mode as described in the following steps:

- When you specify the IP data from the console terminal, the IP address becomes the in-band address of the switch. BootP requests are not broadcast. You can manage the switch using this in-band IP address.
- When you do not specify the in-band IP address from the console terminal, the switch broadcasts BootP requests until it receives a BootP reply containing an in-band IP address. If the switch does not receive a BootP reply that contains an in-band IP address within 10 minutes, the switch uses the last in-band IP address it received from a BootP server. This IP information is displayed in the Last BootP column.

If the IP address specified as the in-band IP address is not currently in use, these actions take effect immediately. If an IP address is currently in use, these actions take effect only after the switch is reset or power cycled.

Default BootP setting

The default operational mode for BootP on the switch is BootP, 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).

Asset ID configuration

Asset ID provides inventory information for the switch, stack, or each unit within a stack. An Asset ID consists of an alphanumeric string of up to 32 characters in length for the switch or stack. You can configure the Asset ID to record your company specific asset tracking information, such as an asset tag affixed to the switch. You can configure the Asset ID with CLI commands, or with EDM.

Video Surveillance script

Video Surveillance (VS) script allows you to automatically configure parameters for the switch using the **`run vs`** command. The configuration is optimized for solutions with Video Surveillance (VS), where the switch is set up in a best practices solution with VS.

A new CLI command, `run vs`, invokes the script to set VLAN IDs, IP addresses, DHCP servers scopes, and enables DHCP Server and IP routing.

For more information running the VS script, see Run the VS script on page 127.

Extreme Networks 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 42) 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 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 is correctly updated.

When Energy Saver is active and you replace a unit, that unit will not be in energy save 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 6: Energy savings

Switch model	Typical power consumption in Normal Mode (in watts)	Typical power consumption in Energy Saver (in watts)	Savings per switch (in Watts)	Savings per port (in Watts)
ERS3626GTS	18.28	14.58		
ERS3626GTS-PWR+[1]	30.17	27.65		
ERS3650GTS	35.50	26.95		
ERS3650GTS-PWR+[1]	46.11	41.61		
[1]The power consumption values in this table can vary by up to 10%. Power consumption values can differ if a switch operates at different voltages. Power supplies operating at higher voltages are generally more efficient.				

Configure with IP Office Script

Before you begin

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

Extreme Networks recommends that the run ipoffice CLI commands are executed on an switch operating in a factory default state.

Procedure

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

   ```
   run ipoffice [verbose]
   ```

Example

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

```
Switch>run ipoffice

% The Voice VLAN ID has been set to 42
% The Voice VLAN Gateway IP address has been set to 192.168.42.254
% The Voice VLAN Gateway IP network mask has been set to 255.255.255.0
% The Data VLAN ID has been set to 44
% The Data VLAN IP address has been set to 192.168.44.254
% The Data VLAN IP network mask has been set to 255.255.255.0
% ------------------------------------------------------------------
% IP Offie LAN port is et to plug into switch port 1
% Gateway Modem-Router port is set to plug into switch port 2
% ------------------------------------------------------------------
% Default IP Route set to 192.168.44.2 (Gateway Modem-Router interface)
% IP Office Call-Server IP address is set to 192.168.42.1
% IP Office File-Server IP address is set to 192.168.42.1
% ** Switch QoS and Unified Communications policies setup and saved **
% ** IP Office solution automated switch setup complete and saved **
% ------------------------------------------------------------------
% To manage this Extreme Networks switch, enter 192.168.44.254 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 Networks switch for optimal operation with IP Office. ***
*** ---------------------------------------------------***
*** The values in [] are the default values, you can   ***
*** input alternative values at any of the prompts.    ***
*** Warning: This script may delete previous settings. ***
*** If you wish to terminate or exit this script       ***
*** enter ^C <control-C> at any prompt.                ***
*********************************************************
Voice VLAN ID [42] :
% The Voice VLAN ID has been set to 42
Data VLANI ID [44] :
Voice VLAN Gateway IP Address [192.168.42.254] :10.10.42.254
Voice VLAN Gateway IP Mask [255.255.255.0] :
% The Voice VLAN Gateway IP address has been set to 10.10.42.254
% The Voice VLAN Gateway IP network mask has been set to 255.255.255.0
% The Data VLAN ID has been set to 44
Data VLAN Gateway IP Address [192.168.44.254] :10.10.44.254
Data VLAN Gateway IP Mask [255.255.255.0] :
% The Data VLAN IP address has been set to 10.10.44.254
% The Data VLAN IP network mask has been set to 255.255.255.0
% IP Office LAN port is set to plug into switch port 1
% Gateway Modem-Router port is set to plug into switch port 2
```

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

FA LLDP extensions

The Fabric Attach (FA) TLVs described in this section are implemented as extensions to the LLDP standard, using the flexible extension mechanism supported by the standard. These TLVs use TLV type 127 as described in the 802.1ab (LLDP) standard.

Extreme Networks Fabric Attach Element TLV

With the Extreme Networks 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 switch 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 Extreme Networks FA Element TLV contains the following data:

- FA Element Type – indicates element capabilities
- FA Element Management VLAN – identifies the management VLAN
- FA Element System ID - unique system identifier used to support element discovery and tracking.
- FA Element State Data - supports the exchange of element state information

The FA Element TLV is included in all LLDPDUs when the FA service is enabled and when the port-level transmission flags associated with this TLV are enabled.

You can view the FA port settings but you cannot update them through the LLDP support. Use the `fa port-enable` command to update the FA port settings.

With the FA service enabled, LLDPDUs containing proprietary Extreme Networks TLVs are transmitted on links that may or may not have Extreme Networks 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 Extreme Networks LLDP TLVs are handled. The other proprietary Extreme Networks TLVs are only included in LLDPUs generated on links that have recognized Extreme Networks elements, specifically Extreme Networks telephony gear, at the far end.

Extreme Networks FA I-SID/VLAN Assignment TLV

With the Extreme Networks FA I-SID/VLAN Assignment TLV, an FA Proxy or FA Client distributes I-SID/VLAN assignments to the FA Server. This information is received, processed and stored by the receiving device so that it is immediately accessible for internal applications.

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 an LLDPDU when complementary FA element devices (FA Proxy, FA Server, or FA Client) are directly connected. The associated port-level transmit flags must be enabled as well.

The Organizationally Specific Extreme Networks FA I-SID/VLAN Assignment TLV contains the following data:

- VLAN ID – identifies the VLAN component of the I-SID-to-VLAN mapping
- I-SID – identifies the I-SID component of the I-SID-to-VLAN mapping
- Status – contains information related to the processing of the I-SID-to-VLAN mapping

Multiple I-SID/VLAN assignments may 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 support 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 may also reject proposed I-SID/VLAN assignments. In this case, the assignment state is updated to rejected.

Extreme Networks TLV Transmit Flags

With the transmit flags, you can choose on a port-level basis, which LLDP TLVs (including the Extreme Networks TLV 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 Extreme Networks TLVs (the PoE Conservation Levels TLV default depends on the devices's PoE support) on all ports. The transmit flags for the FA Element and FA I-SID/VLAN Assignment TLVs default to enabled on the switch, 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 System using CLI

Set the Read-Only and Read-Write Passwords

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   username <username> <password> [<ro | rw>]
   ```

3. To set the username to system default, enter the following command:

4. ```
   default username [<ro | rw>]
   ```

Variable definitions

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

Variable	Value
<username> <password>	Enter your user name for the first variable, and your password for the second variable. The default user name values are RO for read-only access and RW for read/write access.
ro|rw	Specifies that you are modifying the read-only (ro) user name or the read-write (rw) user name. The ro/rw variable is optional. If it is omitted, the command applies to the read-only mode.

IP Office Script

You can use the IPOffice script to quickly and automatically configure parameters for the switch. The configuration is optimized for solutions with IP Office supporting approximately 2 to 384 users on the switch platform, and more when stacking is used.

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

Table 7: Default parameters for IPOffice script

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

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

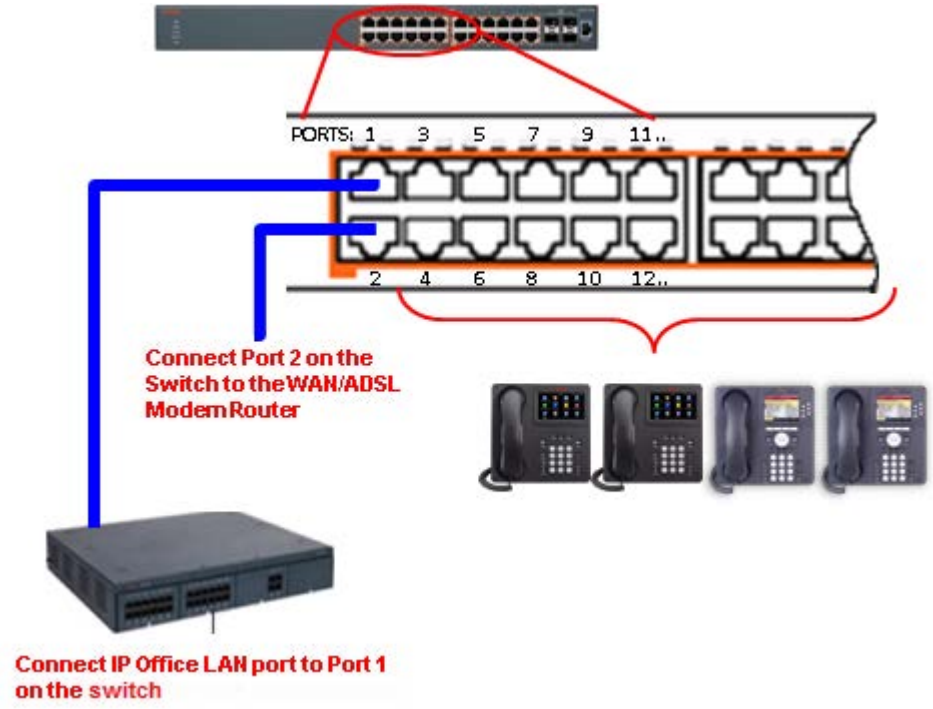


Figure 6: Connecting IP Office, IP Phones and other devices

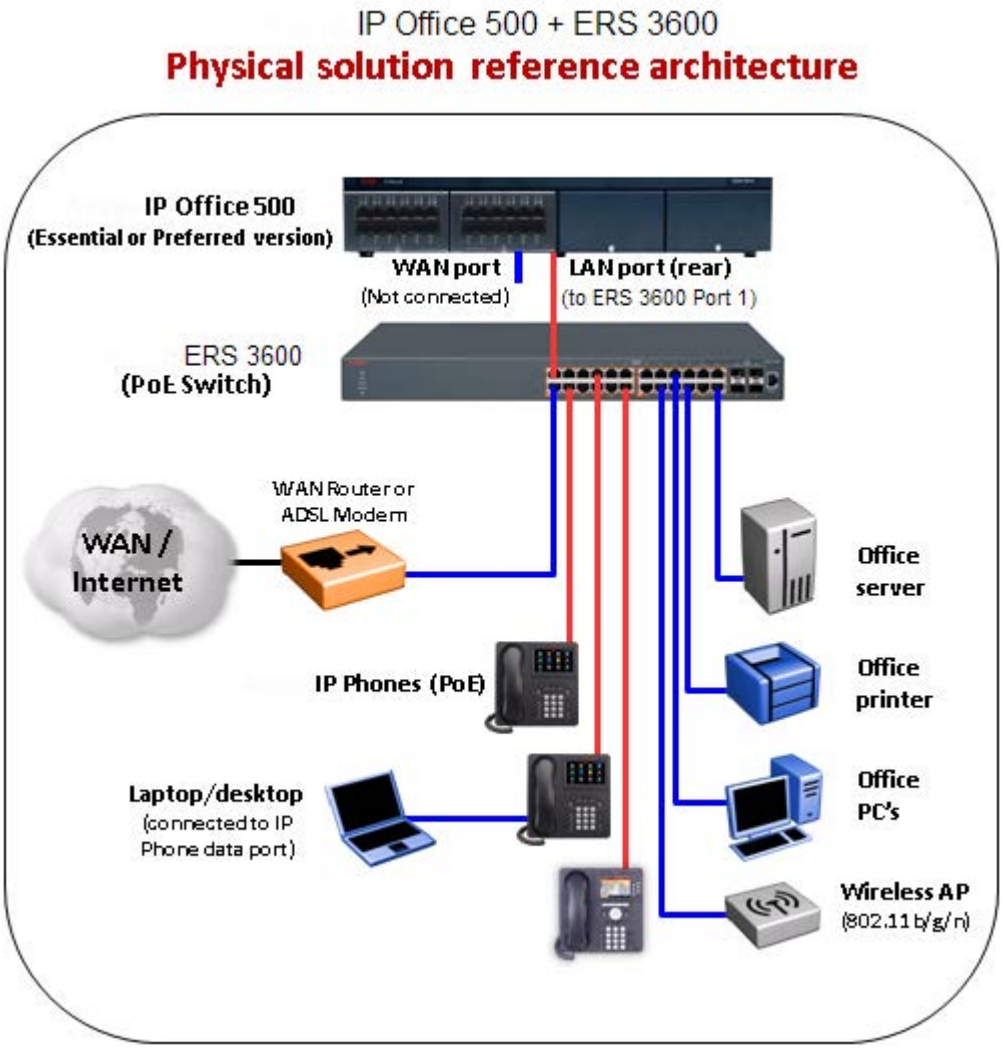


Figure 7: IP Office physical solution reference diagram

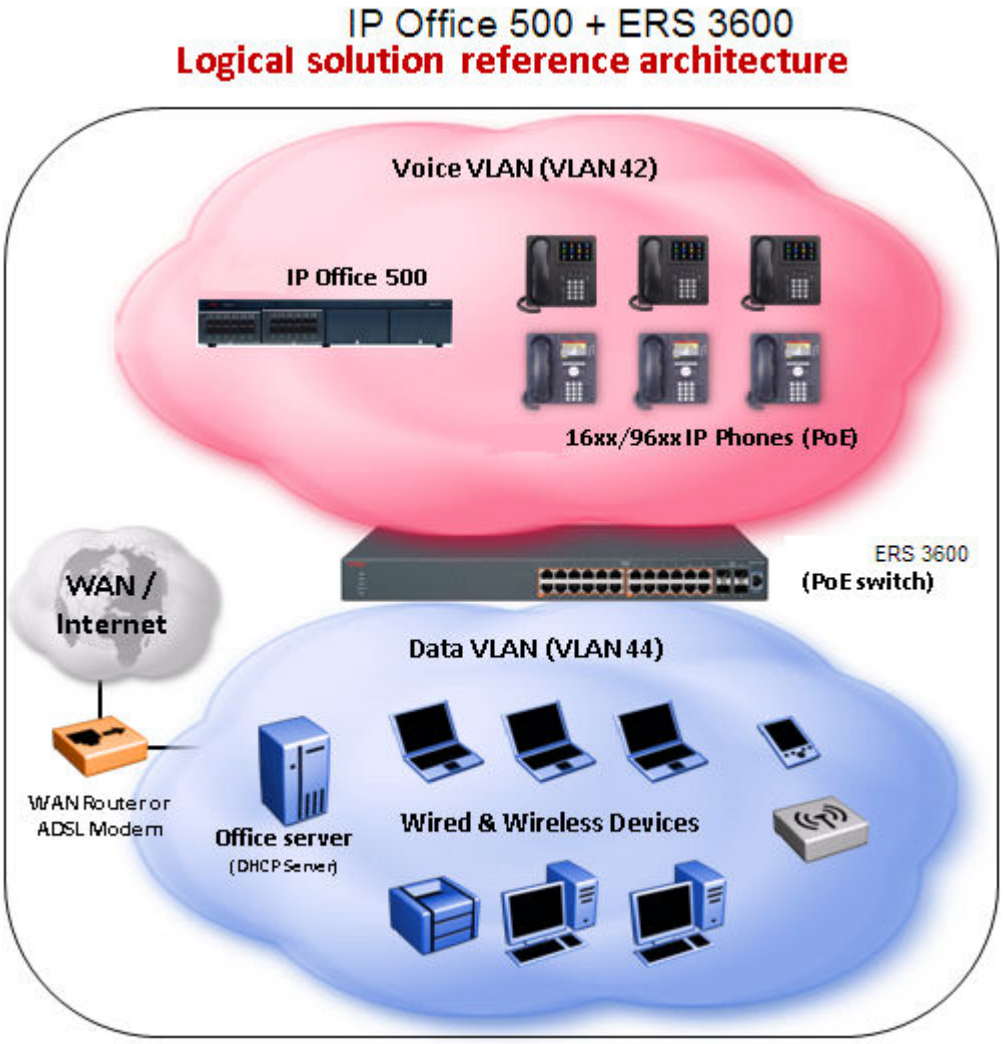


Figure 8: IP Office logical solution reference diagram

Configure with IP Office Script

Before you begin

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

Extreme Networks recommends that the run ipoffice CLI commands are executed on an switch operating in a factory default state.

Procedure

1. To enter User EXEC mode, log on to the switch.

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

   ```
   run ipoffice [verbose]
   ```

Example

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

```
Switch>run ipoffice

% The Voice VLAN ID has been set to 42
% The Voice VLAN Gateway IP address has been set to 192.168.42.254
% The Voice VLAN Gateway IP network mask has been set to 255.255.255.0
% The Data VLAN ID has been set to 44
% The Data VLAN IP address has been set to 192.168.44.254
% The Data VLAN IP network mask has been set to 255.255.255.0
% ------------------------------------------------------------------------
% IP Offie LAN port is et to plug into switch port 1
% Gateway Modem-Router port is set to plug into switch port 2
% ------------------------------------------------------------------------
% Default IP Route set to 192.168.44.2 (Gateway Modem-Router interface)
% IP Office Call-Server IP address is set to 192.168.42.1
% IP Office File-Server IP address is set to 192.168.42.1
% ** Switch QoS and Unified Communications policies setup and saved **
% ** IP Office solution automated switch setup complete and saved **
% ------------------------------------------------------------------------
% To manage this Extreme Networks switch, enter 192.168.44.254 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 Networks switch for optimal operation with IP Office. ***
*** ---------------------------------------------------***
*** The values in [] are the default values, you can   ***
*** input alternative values at any of the prompts.    ***
*** Warning: This script may delete previous settings. ***
*** If you wish to terminate or exit this script       ***
*** enter ^C <control-C> at any prompt.                ***
*********************************************************
Voice VLAN ID [42] :
% The Voice VLAN ID has been set to 42
Data VLANI ID [44] :
Voice VLAN Gateway IP Address [192.168.42.254] :10.10.42.254
Voice VLAN Gateway IP Mask [255.255.255.0] :
% The Voice VLAN Gateway IP address has been set to 10.10.42.254
% The Voice VLAN Gateway IP network mask has been set to 255.255.255.0
% The Data VLAN ID has been set to 44
Data VLAN Gateway IP Address [192.168.44.254] :10.10.44.254
Data VLAN Gateway IP Mask [255.255.255.0] :
% The Data VLAN IP address has been set to 10.10.44.254
% The Data VLAN IP network mask has been set to 255.255.255.0
% IP Office LAN port is set to plug into switch port 1
% Gateway Modem-Router port is set to plug into switch port 2
IP Route to Gateway Modem-Router (Internet/WAN) [192.168.44.2] :10.10.44.99
% Default IP Route set to 10.10.44.99 (Gateway Modem-Router interface)
IP Office Call-Server IP address [192.168.42.1] :10.10.42.200
% IP Office Call-Server IP address is set to 10.10.42.200
IP Office File-Server IP address [192.168.42.1] :10.10.42.200
% IP Office File-Server IP address is set to 10.10.42.200
% ** Switch QoS and Unified Communications policies setup and saved **
```

```
% ** IP Office solution automated switch setup complete and saved **
% ------------------------------------------------------------------------
% To manage this Extreme Networks switch, enter 10.10.44.254 in your Web browser.
% ------------------------------------------------------------------------
```

Upgrading Software using the CLI

You can download the switch software image that is in nonvolatile flash memory. To download the software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the switch must have an IP address.

Caution:

Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

Upgrade Switch Software

You can upgrade both the switch software image and the diagnostics image.

Important:

Unless the no-reset option is selected, the system resets after downloading a new image.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   download [address <ip>] {image <image-name>|image-if-newer <image-
   name>|diag <filename> [no-reset] | poe-module-image }
   ```

   Important:

   You can use the **`download`** command without parameters. The system displays the most recently used TFTP server IP address and file name; if you still want to use these, press `Enter`. You can also change these.

   The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Take care not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

   When the download process is complete, the switch automatically resets and the new software image initiates a self-test, unless the no-reset option is selected. The system returns a message after successfully downloading a new image.

   During the download process, the switch is not operational. You can monitor the progress of the download process by observing the LED indications.

Example

The following figure provides a sample output of the **download** command.

```
switch:1#download
Address [0.0.0.0]:192.0.2.1
Filename [image-file.img] :
Finished Upgrading Image
Rebooting
```

Variable definitions

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

Variable	Value
address <*ip*>	Specifies the IP address of the TFTP server you want to use. **Important:** If this parameter is omitted, the system goes to the server specfied by the **tftp-server** command.
image <*image-name*>	Enter the name of the software image you want to download.
image-if-newer <*image-name*>	Enter the name of the software image of the newer version you want to download.
diag <*filename*>	Enter the name of the diagnostic image you want to download.
no-reset	Download the specified software without resetting the unit.
poe-module-image	Specifies the name of the PoE image file.

Show Software Status

You can display the currently loaded and operational switch or stack software status for both agent and diagnostic loads. You can use the **show boot** CLI command and variables to display the agent or diagnostic load status individually, or combined.

Display the Agent and Diagnostic Software Load

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

Procedure

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

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

Example

The following figure provides a sample output of the **show boot** command.

```
Switch>show boot
Unit  Agent Image Active Image Diag Image Active Diag
----- ----------- ------------ ---------- -----------
1     6.1.0.043   6.1.0.043    6.0.0.3    6.0.0.3
2     6.1.0.043   6.1.0.043    6.0.0.3    6.0.0.3
3     6.1.0.043   6.1.0.043    6.0.0.3    6.0.0.3
4     6.1.0.043   6.1.0.043    6.0.0.3    6.0.0.3
* - Stack requires reboot for new Active Image to be made operational.
# - Stack requires reboot for new Diag to be made operational.
```

Variable definitions

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

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

Reset the Switch to Default Configuration

Reset the switch to its factory default configuration.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

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

   `restore factory-default [ –y | force]`

3. The `-y` or `force` parameter instructs the switch not to prompt for confirmation. If the `-y` or `force` parameter is not included in the command, the following message appears:`Warning the switch will be reset to factory default configurationDo you wish to continue (y/n)?`

   Enter `y` to restore the swtich to default.

Configuring a TFTP Server

Set TFTP Parameters

You can display the IP address of the TFTP server and assign an IP address to the TFTP server.

For procedures to copy a configuration file to the TFTP server, or copy a configuration file from the TFTP server to the switch to use to configure the switch, see Using CLI and EDM on Ethernet Routing Switch 3600 Series.

Display the default TFTP Server

Display the IP address of the server used for all TFTP-related transfers.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show tftp-server
   ```

Example

The following figure provides a sample output of the **`show tftp-server`** command.

```
switch#show tftp-server
TFTP Server IP address: 172.16.3.2
```

Assign or Clear the TFTP Address

Assign or clear the address for the switch to use for TFTP services.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
<A.B.C.D>	Specifies the dotted-decimal IP address of the server you want to use for TFTP services in the format XXX.XXX.XXX.XXX.
<WORD>	Specifies the IPv6 address of the server you want to use for TFTP services.
no	Clears the TFTP server IP address to 0.0.0.0.
default	Sets the TFTP server IP address to 0.0.0.0.

Using Configuration Files

Configuration files allow the administrator to change switch configuration quickly. You can display, store, and retrieve configuration files, and save the current configuration.

The Configuration management feature lets you store and retrieve the configuration parameters of the switch to a TFTP server and retrieve the parameters to automatically configure a replacement switch. This feature supports two different methods for managing system configuration files:

- binary configuration files
- ASCII configuration files

Before you change the switch configuration, you can use the **`show running-config`** command to view the current configuration. The command displays only those parameters that differ from the default switch configuration. If you want to view the entire configuration, you must use the verbose qualifier to view the configuration for a specific feature.

A configuration file obtained from a stand-alone switch can only be used to configure other stand-alone switches that have the same firmware revision and model type as the donor stand-alone switch.

The following parameters are not saved to the configuration file:

- Configuration Image Filename
- Terminal settings (speed, width, length)

For more information, see Using CLI and EDM on Ethernet Routing Switch 3600 Series.

Enable or Disable AUR

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable AUR, enter the following command:

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

3. To disable AUR, enter the following command:

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

4. To default AUR, enter the following command:

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

Display the Current Configuration

Use this procedure to display the current configuration of the switch or 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 received 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 figure provides a sample of the **`show running-config`** command with the MLT value.

```
Switch# show running-config module mlt
 Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 3626GTS-PWR+
! Software version = v6.1.0.039
!
! Displaying only parameters different to default
!================================================
enable
configure terminal
!
! *** MLT (Phase 1) ***
!
no mlt
mlt 1 name "Trunk #1" enable member 11-14
mlt 1 bpdu single-port
mlt 1 loadbalance advance
mlt 2 name "Trunk #2" enable member 21-24
!
! *** MLT (Phase 2) ***
!
mlt spanning-tree 1 stp learning fast
mlt spanning-tree 2 stp learning disable
```

```
Switch#show running-config verbose
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 3626GTS-PWR+
! Software version = v6.1.0.039
```

```
!
! Displaying all switch parameters
!======================================================
enable
configure terminal
!
!
! *** CORE ***
!
! *** RADIUS ***
!
! *** RADIUS Dynamic Server ***
!
! *** TACACS+ ***
!
! *** SNMP ***
!
! *** IP  ***
!
! *** IP Manager ***
!
! *** ASSET ID ***
!
! *** System Logging ***
!
! *** STACK ***

! *** Custom Banner ***
!
! *** SSH ***
!
! *** SSL ***
!
! *** SSHC ***
!
! *** STPG (Phase 1) ***
!
! *** LACP (Phase 1) ***
!
! *** VLAN ***
!
! *** 802.1ab ***
!
! *** 802.1AB MED Voice Network Policies ***
!
! *** QOS ***
!
! *** RMON ***
!
! *** EAP ***
!
! *** EAP Guest VLAN ***
!
! *** EAP Fail Open VLAN ***
!
! *** EAP Voip VLAN ***
!
! *** Interface ***
!
! *** Rate-Limit ***
!
! *** MLT (Phase 1) ***
!
! *** MAC-Based Security ***
!
```

```
! *** LACP (Phase 2) ***
!
! *** ADAC ***
!
! *** STP (Phase 2) ***
!
!! *** Port Mirroring ***
!
! *** VLAN Phase 2***
!
! *** MLT (Phase 2) ***
!
! *** PoE ***
!
poe power-mode high-power-budget
poe poe-power-usage-threshold 80
poe poe-pd-detect-type 802dot3at
interface Ethernet ALL
poe poe-shutdown port 1
poe poe-priority port 1 low
poe poe-limit port 1 1
poe poe-power-up-mode port 1 high-inrush
!
exit
!
! *** RTC ***
!
! ***Energy Saver ***
!
! *** AUR ***
!
stack auto-unit-replacement enable
stack auto-unit-replacement config save enable
!
! *** AAUR ***
!
stack auto-unit-replacement-image enable
!
! *** L3 ***
!
! *** IPV6 ***
!
! *** MLD ***
!
! *** 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 ---
!
! *** VLACP ***
!
```

```
! *** DHCP Relay ***
!
! *** L3 Protocols ***
!
! --- IP Directed Broadcast ---
!
! --- Proxy ARP ---
!
! --- UDP Broadcast Forwarding ---
!
! --- Route Policies ---
!
! --- RIP ---
!
! *** ARP INSPECTION ***
!
! *** IP SOURCE GUARD ***
!
! *** IGMP ***
!
! *** STACK MONITOR ***
!
! *** SLPP-guard ***
!
! *** DHCP Server ***
!
! *** SLAMON ***
!
! *** STORM CONTROL ***
!
! *** Fabric Attach ***
!
fa zero-touch
fa proxy
no fa standalone-proxy
no fa uplink
fa timeout 240
no fa extended-logging
fa zero-touch-option auto-port-mode-fa-client
no fa zero-touch-option auto-trusted-mode-fa-client
no fa zero-touch-option auto-pvid-mode-fa-client
fa zero-touch-option ip-addr-dhcp
no fa zero-touch-option auto-client-attach
fa port-enable ALL
fa message-authentication ALL key-mode strict
```

Variable definitions

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

Variable	Value
verbose	Displays entire configuration, including defaults and non-defaults.
module <*value*>	Displays configuration of an application for any of the following parameters: *[802.1AB][aaur] [adac] [arp-inspection] [asset-id][aur][banner] [core] [dhcp-relay] [dhcp-server][dhcp-snooping] [eap] [igmp][interface] [ip] [ip-source-guard] [ipmgr] [ipv6] [l3] [l3-protocols] [lacp] [logging] [mac-security] [mlt] [poe] [port-*

Table continues…

Variable	Value
	mirroring] [qos] [rate-limit] [rmon] [rtc] [slamon][snmp] [ssh] [ssl] [stack][stkmon][storm-control] [stp] [vlacp] [vlan]

Configuring Telnet

Set Telnet Access

You can access CLI through a Telnet session. To access CLI remotely, the management interface must have an assigned IP address and remote access must be enabled. You can log on to the switch using Telnet from a terminal that has access to the switch.

Important:

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

You can view the Telnet-allowed IP addresses and settings, change the settings, or disable the Telnet connection.

Display Telnet Access Current Settings

Display the current settings for Telnet access.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show telnet-access
   ```

Example

The following figure displays sample output for the **`show telnet-access`** command.

```
Switch#show telnet-access
TELNET Access:       Enabled
Login Timeout:       1 minute(s)
Login Retries:       3
Inactivity Timeout:  15 minute(s)
Event Logging:       All
Allowed Source IP Address    Allowed Source Mask
-------------------------    -------------------
1   0.0.0.0                     0.0.0.0
2   255.255.255.255             255.255.255.255
3   255.255.255.255             255.255.255.255
4   255.255.255.255             255.255.255.255
5   255.255.255.255             255.255.255.255
6   255.255.255.255             255.255.255.255
7   255.255.255.255             255.255.255.255
8   255.255.255.255             255.255.255.255
9   255.255.255.255             255.255.255.255
```

```
10  255.255.255.255             255.255.255.255
11  255.255.255.255             255.255.255.255
12  255.255.255.255             255.255.255.255
13  255.255.255.255             255.255.255.255
14  255.255.255.255             255.255.255.255
----More  (q=Quit, space/return=Continue)----
```

Configure Telnet Access

Configure the Telnet connection that is used to manage the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

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

   ```
   [no] [default] telnet-access [enable|disable] [login-timeout <1–10>]
   [retry <1–100>] [inactive-timeout <0–60>] [logging {none|access|
   failures|all}] [source-ip <1–10> <A.B.C.D>[mask <A.B.C.D>]]
   ```

Variable definitions

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

Variable	Value
enable | disable	Enables or disables Telnet connections
login-timeout *<1–10>*	Specifies the time in minutes that you want to wait between an initial Telnet connection and acceptance of a password, before closing the Telnet connection; enter an integer between 1 and 10.
retry *<1–100>*	Specifies the number of times that the user can enter an incorrect password before closing the connection; enter an integer between 1 and 100.
inactive-timeout *<0–60>*	Specifies in minutes how long to wait before closing an inactive session; enter an integer between 0 and 60.
logging *none* | *access* | *failures* | *all*	Specifies what types of events you want to save in the event log: • All — Saves all access events in the log: - Telnet connect — indicates the IP address and access mode of a Telnet session - Telnet disconnect — indicates the IP address of the remote host and the access mode, due to either a log off or inactivity. - Failed Telnet connection attempts — indicates the IP address of the remote host that is not on

Table continues…

Variable	Value
	the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password. • none — No Telnet events are saved in the event log. • access — Connect and disconnect events are saved in the event log. • failure — Only failed Telnet connection attempts are saved in the event log.
source-ip *<1–10> <A.B.C.D>[mask <A.B.C.D>]*	Specifies up to 10 IP address from which connections are allowed. Enter the IP address either as an integer or dotted-decimal notation (A.B.C.D in the format XXX.XXX.XXX.XXX). Specifies the subnet mask from which connections are allowed; enter the IP mask in dotted-decimal notation (A.B.C.D in the format XXX.XXX.XXX.XXX) **Important:** These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see Configuring Security on Ethernet Routing Switch 3600 Series.
no telnet-access [source-ip [<1–10>]]	Disables the Telnet connection. When you do not use the optional parameter, the source-up list is cleared, meaning that the 1st index is set to 0.0.0.0/0.0.0.0 and the 2nd to 10th indexes are set to 255.255.255.255/255.255.255.255. When you do specify a source-ip value, the specified pair is set to 255.255.255.255/255.255.255.255. **Important:** These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see Configuring Security on Ethernet Routing Switch 3600 Series.
default	Sets the Telnet settings to the default values.

Ping an IP Device

You can ping a device to test the connection between a switch and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address does not respond.

Before you begin

The local IP address must be configured before issuing the **ping** command.

Procedure

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

   ```
   ping <IP_address>
   ```

   where <IP_address> is an IPv4 or IPv6 address.

Example

The following figure shows a sample ping response.

```
Switch>ping 120.16.125.10
Host is reachable
```

Variable definitions

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

Variable	Value
<A.B.C.D > | *<dns_host_name>* | *<WORD>*	Specifies the IP address, DNS host name, or IPv6 address of the unit to test.
datasize*<64–4096>*	Specifies the size of the ICMP packet to be sent. The data size range is from 64 to 4096 bytes.
{count *<1–9999>}* | continuous	Sets the number of ICMP packets to be sent. The continuous mode sets the ping running until the user interrupts it by entering Ctrl-C.
{timeout |-t} *<1–120>*	Sets the timeout using either the timeout or -t parameter, followed by the number of seconds the switch must wait before timing out.
interval*<1–60>*	Specifies the number of seconds between transmitted packets.
debug	Provides additional output information such as ICMP sequence number and trip time.
source*<A.B.C.D>*	Specifies the source IP address of the packet. Must be a configured address on the switch.
ttl*<0–255>*	Specifies the maximum hop limit for the packet. Range of 0 to 255.

Setting Boot Parameters using CLI

You can restart the switch and configure BootP using CLI.

Perform a Soft-start of the Switch

Use this command to perform a soft-start of the switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To perform a soft-start of the switch, enter the following command:

   ```
   boot [default]
   ```

Variable definitions

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

Variable	Value
default	Restores switch to factory-default settings after restarting.

Configure BootP on the Current Instance of the Switch or Server

Use this command to configure BootP on the current instance of the switch or server, as the default ip, the last known address, never, or always.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To configure BootP on the current instance of the switch or server, enter the following command:

   ```
   [no] [default] ip bootp server {default-ip|last|disable|always]
   ```

Variable definitions

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

Variable	Value
default-ip|last|disable|always	Specifies when to use BootP: • default-ip — use BootP or the default IP • last — use BootP or the last known address • disable — never use BootP • always — always use BootP DEFAULT: default-ip

Table continues…

Variable	Value
no	Disables the BootP server
default	Sets the BootP server status to BootP or Default IP
BootP Request Mode	BootP, DHCP or Default IP

Configuring AUR

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

Display AUR

Use this procedure to displays the current AUR settings.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

```
switch#show stack auto-unit-replacement
Auto Unit Replacement Auto-Resorte: Enabled
Auto Unit Replacement Auto-Save:   Enabled

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

Enable or Disable AUR

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable AUR, enter the following command:

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

3. To disable AUR, enter the following command:

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

4. To default AUR, enter the following command:

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

Enable or Disable AUR Configuration Saves

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

Before you begin

AUR requires a stack configuration

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To enable AUR automatic configuration saves, enter the following command:

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

3. To disable AUR automatic configuration saves, enter the following command:

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

Restore AUR Saved Configuration

Use this procedure to restore the AUR saved configuration to a non-base unit.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Note:

Use the base unit console to enter this command.

Save AUR Configuration

Use this procedure to save the configuration of the selected non-base unit to the base unit, regardless of the state of the AUR feature.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

Note:

Use the base unit console to enter this command.

3. Press Enter.

Remove a Unit MAC Address from AUR Cache

Before you begin

Remove the unit from the stack.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enter the following command:

```
stack auto-unit-replacement remove-mac-address <1-8>
```

Configuring AAUR

Use CLI procedures in the following sections 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.

Setting Stack Forced Mode

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

Enable or Disable Stack Forced Mode

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

Before you begin

Stack Forced Mode requires a stack configuration of two units.

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable Stack Forced Mode, enter the following command:

   ```
   stack forced-mode
   ```

3. To disable Stack Forced Mode, enter the following command:

   ```
   no stack forced-mode
   ```

4. To default Stack Forced Mode, enter the following command:

   ```
   default stack forced-mode
   ```

   The default is disabled.

Variable definitions

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

Variable	Value
no	Disables stack forced-mode

Display Stack Forced-mode

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

Before you begin

Stack Forced Mode requires a stack configuration of two units.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

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

   ```
   show stack forced-mode
   ```

Example

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

```
switch(config)#show stack forced-mode
Forced-Stack Mode: Disabled
Device is not currently running in forced stack mode.
```

Shutting down and Resetting the Switch

Shut down the Switch

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Variable definitions

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

Variable	Value
force	Forces the shutdown without confirmation.
minutes-to-wait<*1–60*>	Specifies the number of minutes to wait before the shutdown occurs. DEFAULT: 10
cancel	Cancels a scheduled shutdown any time during the time period specified by the *minutes-to-wait <1–60>* parameter.

Reload Remote Devices

Use this procedure to disable auto saving configuration changes, and safeguard against a configuration error when you perform dynamic configuration changes on a remote switch. If you make an error while configuring a remote switch that results in the loss of connectivity (for example, an error in the IP address, VLAN, and others), the reload loads the last saved configuration to re-establish connectivity.

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

Before you begin

This procedure is intended to be used by system administrators to configure remote devices and reset them when the configuration is complete. The configuration is not explicitly saved after the **reload** command is issued. This means that any configuration changes must be explicitly saved before the switch reloads.

Caution:

You must perform a timed reload command before making dynamic configuration changes to safeguard against the loss of remote connectivity.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

The following example shows use of the **reload** command as a safeguard during dynamic configuration changes:

1. Enter **reload force minutes-to-wait 30** to instruct the switch to reboot in 30 minutes and load the configuration from NVRAM. During the 30 minute countdown, autosave of the configuration is disabled.

2. Execute dynamic switch configuration commands. The command take effect immediately and are not saved to NVRAM.
3. Test your configuration changes. If problems occurred, when the 30 minute countdown expires, the switch reboots and loads the previous configuration. If no problems occur, and switch connectivity is maintained, you can perform one of the following tasks before the 30 minute countdown expires:

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

Variable definitions

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

Variable	Value
force	Forces the reload without confirmation.
minutes-to-wait<*1–60*>	Specifies the number of minutes to wait before the reload occurs. DEFAULT: 10
cancel	Cancels a scheduled reload any time during the time period specified by the *minutes-to-wait* <*1–60*> parameter.

Configure LEDs to blink on the Display Panel

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   blink-leds [off | time <1–10> | unit <1–8>]
   ```

Variable definitions

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

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

Table continues…

Variable	Value
unit *<1–8>*	Specifies the unit number. RANGE: 1 to 8 units

Configure the Operational Mode of the Stacking Ports

Use this procedure to configure the operational mode of the stacking ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   stacking—ports mode stacking
   ```

Display Operational Mode of the Stacking Ports

Use this procedure to display the operational mode of the stacking ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show stacking-ports mode
   ```

Example

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

```
Switch(config)#show stacking-ports mode
Current stacking-ports mode: Stacking Mode
Next stacking-ports mode: Stacking Mode
Next mode will be applied after reset
```

Managing Ethernet Ports using CLI

Autosense and Autonegotiate

The switch is an autosensing and autonegotiating device.

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

Autosensing is used when the attached device is not capable of autonegotiation or is using a form of autonegotiation that is not compatible with the IEEE 802.3u standard. In this case, because it is not possible to sense the duplex mode of the attached device, the switch reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the switch, the ports negotiate down from 1000 Mb/s speed and full-duplex mode and from 100 Mb/s speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

Advertising Custom Autonegotiation

Custom Autonegotiation Advertisements (CANA) lets you customize the capabilities that you advertise. For example, if a port is not capable of 10/100/1000 full duplex operation, the port can be configured to only advertise 10 half-duplex capabilities.

CANA lets you control the capabilities that are advertised by the Ethernet switches as part of the autonegotiation process. In the current software releases, autonegotiation can either be enabled or disabled.

When autonegotiation is disabled, the hardware is configured for a single (fixed) speed and duplex value. When autonegotiation is enabled, the advertisement made by the product is a constant value based upon all speed and duplex modes supported by the hardware.

When autonegotiating, the switch selects the highest common operating mode supported between the switch and its link partner.

In certain situations, it is useful to autonegotiate a specific speed and duplex value. In these situations, the switch can allow for attachment at an operating mode other than its highest supported value.

For example, if the switch advertises only a 100 Mbps full-duplex capability on a specific link, the link goes active only if the neighboring device is also capable of autonegotiating a 100 Mbps full-duplex capability. This prevents mismatched speed and duplex modes if customers disable autonegotiation on the neighboring device.

Important:

The CANA feature is available for 10/100 Ethernet ports of ERS 3626GTS switches (not available for rear ports).

Enable Custom Autonegotiation Advertisement in CLI

You can control the capabilities that are advertised by the Ethernet Routing Switch as part of the auto-negotiation process using the CANA feature. After auto-negotiation is disabled, the hardware is

configured for a single (fixed) speed and duplex value. After auto-negotiation is enabled, the advertisement made by the switch is a constant value based upon all speed and duplex modes supported by the hardware. After auto-negotiating, the switch selects the highest common operating mode supported between it and its link partner.

Display the Current Autonegotiation Advertisements

Use this command to display the current autonegotiation advertisements.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To display the current autonegotiation advertisements, enter the following command:

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

Example

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

Variable definitions

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

Variable	Value
port<*portlist*>	Enter ports for which you want the current autonegotiation advertisements displayed. If you enter more than one port number, separate ports with a comma (,).

Display the Hardware Advertisement Capabilities for the Switch

Use this command to display the hardware advertisement capabilities for the switch.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. To display the hardware advertisement capabilities for the switch, enter the following command:

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

Example

```
switch>show auto-negotiation-capabilities port 1/20-26
Unit/Port   Autonegotiation  Capabilities
```

```
---------   ------------------------------------------------------------------
1/20        10Full 10Half 100Full 100Half
1/21        10Full 10Half 100Full 100Half
1/22        10Full 10Half 100Full 100Half
1/23        10Full 10Half 100Full 100Half
1/24        10Full 10Half 100Full 100Half
1/25        10Full 10Half 100Full 100Half 1000Full              AsymmPause
1/26        10Full 10Half 100Full 100Half 1000Full              AsymmPause
```

Variable definitions

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

Variable	Value
port<*portlist*>	Enter ports for which you want the current autonegotiation capabilities displayed. If you enter more than one port number, separate ports with a comma (,).

Enable or Disable a Port

Important:

You can disable switch ports that are trunk members, if you choose to disable them one by one. If you choose to disable all ports of the unit or stack, the changes can affect the ports belonging to MLTs.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port> or interface vlan <1-4094>
   ```

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

   ```
   [no] shutdown [line <portlist>]
   ```

Example

The following figure provides a sample of the output of the **`shutdown [port <portlist>]`** command.

```
switch(config-if)#shutdown port 6
```

Variable definitions

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

Variable	Value
port <*portlist*>	Specifies the port numbers to shut down or disable. Enter the port numbers you want to disable.

Table continues…

Variable	Value
	Important: If you omit this parameter, the system uses the port number you specified in the **`interface`** command.
no	Specifies the port numbers to enable. Enter the port number you want to enable. **Important:** If you omit this parameter, the system uses the port number you specified in the **`interface`** command.

Configure Port Naming

You can name ports, change the name, clear the name or reset the port name to an empty string.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port> or interface vlan <1-4094>
   ```

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

   ```
   [no] [default] name [port <portlist>] <LINE>
   ```

Variable definitions

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

Variable	Value
port<*portlist*>	Specifies the port numbers to be named. **Important:** If you omit this parameter, the system uses the port number you specified in the **`interface`** command.
<LINE>	Specifies the name of the port using up to 26 alphanumeric characters.
no	Clears the port names and resets the field to an empty string.
default	Clears the port names and resets the field to the default value (an empty string).

Set Port Speed

Set the speed of a port. Ports can be set to a speed of 10 Mb/s, 100 Mb/s, 1000 Mb/s (or 1 GB/s), or auto-negotiated.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port> or interface vlan <1-4094>
   ```

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

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

Variable definitions

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

Variable	Value
default	Sets the speed of the port to the factory default speed.
port *<portlist>*	Specifies the port numbers to configure the speed. Enter the port numbers to be configured. **Important:** If you omit this parameter, the system uses the port number you specified in the **`interface`** command.
10|100|1000|10000|auto	Sets speed to: • 10 — 10 Mb/s • 100 — 100 Mb/s • 1000 — 1000 Mb/s or 1 Gb/s • 10000 — 10000 Mb/s or 10 Gb/s • auto — autonegotiation **Important:** When you set the port speed for autonegotiation, ensure that the other side of the link is also set for autonegotiation.

Specify Duplex Operation for a Port

Specify duplex operation as full-duplex mode , half-duplex mode, or auto-negotiated. You can also reset duplex operation for a port to the factory default duplex value.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port> or interface vlan <1-4094>
   ```

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

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

Variable definitions

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

Variable	Value
port<*portlist*>	Specifies the port number to configure the duplex mode. Enter the port number you want to configure, or ALL to configure all ports simultaneously. **Important:** If you omit this parameter, the system uses the port number you specified in the **`interface`** command.
full|half|auto	Sets duplex to: • full — full-duplex mode • half — half-duplex mode • auto — autonegotiation **Important:** When you set the duplex mode for autonegotiation, ensure that the other side of the link is also set for autonegotiation.
default	Sets the duplex operation for a port to the factory default duplex value.

High speed flow control

The high speed flow control feature lets you control traffic and avoid congestion on the gigabit full-duplex link. If the receive port buffer becomes full, the switch issues a flow-control signal to the device at the other end of the link to suspend transmission. When the receive buffer is no longer full, the switch issues a signal to resume the transmission. You can set the flow control mode to Asymmetric or disabled.

Asymmetric mode

This mode lets the link partner send flow control pause frames to the Gigabit Ethernet port. When a pause frame is received, the receiving port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frame is received.

In this mode, the port is disabled from transmitting pause frames to its link partner. Use this mode when the port is connected to a buffered repeater device.

You can choose a flow control mode with CLI commands.

Enable Flow Control

If you use a Gigabit Ethernet with the switch, you control traffic on this port using the **`flowcontrol`** command.

About this task

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

Note:

You can activate flow control as follows:

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port> or interface vlan <1-4094>
   ```

2. To configure flow control on Gigabit Ethernet ports, enter the following command:

   ```
   [no] [default] flowcontrol [port <portlist>] {asymmetric | auto | disable}
   ```

Variable definitions

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

Variable	Value
port *<portlist>*	Specifies the port numbers to use for flow control **Important:** If you omit this parameter, the system uses the port number you specified in the **`interface`** command.
asymmetric | auto | disable	Sets the mode for flow control: • asymmetric — enables the local port to perform flow control on the remote port

Table continues…

Variable	Value
	• auto — enables auto-negotiation on the specified port and flow control status will be determined after the auto-negotiation process completes, depending on the currently activated auto-negotiation advertisements • disable — disables flow control on the port DEFAULT:auto
no	Disables flow control on the specified port(s).
default	Sets the flow control to auto, which automatically detects the flow control on the specified port(s).

Configure the MDI/X Setting for Ports

About this task

Use this procedure to configure the MDI/X settings for a copper Ethernet port.

Note:

You need to disable auto-negotiation on the link to be able to configure MDI/X. You can use either of the CLI commands `speed <10 | 100 | 1000 | 10000>` or `duplex <full | half>`.

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port>
   ```

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

   ```
   mdix [port <portlist>] { auto | forceAuto | normal | xover }
   ```

3. Press Enter.

Example

```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch+(config)#interface ethernet all
Switch+(config-if)#mdix port 1/1 xover
```

Next steps

The CLI command `show interface verbose` contains a field to display the MDIX mode.

```
Switch>enable
Switch#show interface verbose
Unit/Port:  1/1
    Trunk:
```

```
    Admin Status:  Enable
    Oper Status:   Up
    EAP Oper Status:   Up
    VLACP Oper Status: Down
    STP Oper Status:  Learning
    Link Up
    Last Change: 0 day(s), 00h:00m:25s ago
    LinkTrap:  Enabled
    Link Autonegotiation: Enabled
    Link Speed: 100Mbps
    Link Duplex: Full-Duplex
    Flow Control: Disable
    Energy Saver: Disabled
    Energy Saver Oper Staus: No Power Saving
    BPDU-guard (BPDU Filtering): Disabled
    BPDU-guard (BPDU Filterig) Oper Staus: N/A
    SLPP-guard: Disabled
    SLPP-guard Oper Status: N/A
    Mdix Mode: Xover
Unit/Port:  1/2
    Trunk:
    Admin Status:  Enable
...
```

If a port has an MDI/X setting that is not the default (auto), the CLI command `show running-config` displays the MDI/X configuration.

```
Switch>enable
Switch#show running-config
...
!
!
! *** Interface ***
!
interface Ethernet ALL
auto-negotiation-advertisements port 1/47-48,2/47-48 1000-full asymm-pause-frame
mdix port 1/1 xover
exit
!
...
```

Variable definitions

Use the data in the following table to use the **mdix** command.

Variable	Value
port <portlist>	Specifies the port(s) to be configured.
auto	Sets the port(s) to auto-MDIX when autonegotiation is enabled.
forceAuto	Specifies auto-MDIX always, even when autonegotiation is disabled.
normal	Specifies the standard behavior when autonegotiation is disabled. A port from a switch links up with another switch only using crossover cables, while end devices connect with a straight cable.
xover	Specifies that two switches link up with straight cables, while end devices connect with crossover cables.

Manage Power over Ethernet using CLI

Configuring PoE Switch Parameters

You configure power parameters for each Ethernet Routing Switch 3600 Series that supports PoE with CLI. You can configure the DC power source and the power usage with this management system.

Set the Method to Detect Power Devices

Set the method the PWR+switch uses to detect the power devices connected to the front ports.

You must ensure that this setting is the correct one for the IP appliance you use with the switch. Please note this setting applies to the entire switch, not port-by-port. So, you must ensure that this setting is configured correctly for all the IP appliances on a specified switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   poe poe-pd-detect-type [unit <1-8>] {802dot3at |
   802dot3at_and_legacy}
   ```

Variable definitions

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

Variable	Value
802dot3at | 802dot3at_and_legacy	Sets the detection method the switch uses to detect power needs of devices connected to the front ports: • 802dot3at • 802dot3at_and_legacy DEFAULT: 802dot3at_and_legacy **Important:** Ensure that the power detection method you choose for the ERS 3600-PWR+ matches that used by the IP devices you are powering.
unit <1–8>	Set PD detection mode of an unit in stack

Set a Power Usage Threshold

Set a percentage usage threshold above which the system sends a trap for each PWR+switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   poe poe-power-usage-threshold [unit <1-8>] {<1-99>}
   ```

Variable definitions

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

Variable	Value
<1–99>	Specifies the percentage of total available power you want the switch to use prior to sending a trap. DEFAULT: 80%
unit *<1–8>*	Set power usage threshold of an unit in stack

Displaying PoE configuration

You can display the status for the PoE configuration on the PWR+switch.

Display the Current PoE Configuration

Display the current PoE configuration of the PWR+switch, and settings for each PoE port.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show poe-main-status [unit <1-8>]
   ```

Example

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

```
switch#show poe-main-status
PoE Main Status - Stand-alone
--------------------------
Available DTE Power        : 370 Watts
DTE Power Status           : Normal
DTE Power Consumption      : 0 Watts
DTE Power Usage Threshold  : 80 %
PD Detect Type             : 802.3at and Legacy
Power Source Present       : AC Only
AC Power Status            : Present
DC Power Status            : Not Present
```

Important:

The Power Source Present listing displays the current power source for the switch: AC Only.

Display PoE Port Status

Display the administration status, detection status, power limit, port priority, and the PD classification for each port.

The DTE Power Status displays error messages if the port is not providing power. The following messages can appear:

- Detecting — port detecting IP device requesting power
- Delivering power — port delivering requested power to device
- Invalid PD — port detecting device that is not valid to request power
- Power Denied — power disabled from port because of port setting and demands on power budget
- Overload — power disabled from port because port is overloaded
- Test — port in testing mode
- Error — none of the other conditions apply
- Disabled — the port has been administratively disabled

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

```
3600-1-Doc#show poe-port-status 2
     Admin    Current                  Limit            Power-up
Port Status   Status            Class (Watts) Priority  Mode
---- -------  ----------------- ----- ------- --------  -----------
2    Disable  Disabled            0   0       Low       High Inrush
```

Variable definitions

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

Variable	Value
<portlist>	Enter the ports for which you want to display the status. If you omit this parameter, the system displays all ports.

Display PoE Power Measurement

Display the voltage, current and power values for each powered device connected to each port.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show poe-power-measurement [<portlist>]
   ```

Example

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

```
switch#show poe-power-measurement
Port  Volt(V)  Current(mA)   Power(Watt)
----  -------  -----------   ---------------
1     0.0      0             0.000
2     0.0      0             0.000
3     0.0      0             0.000
4     0.0      0             0.000
5     0.0      0             0.000
6     0.0      0             0.000
7     0.0      0             0.000
8     0.0      0             0.000
9     0.0      0             0.000
10    0.0      0             0.000
11    0.0      0             0.000
12    0.0      0             0.000
13    0.0      0             0.000
14    0.0      0             0.000
15    0.0      0             0.000
16    0.0      0             0.000
17    0.0      0             0.000
18    0.0      0             0.000
19    0.0      0             0.000
20    0.0      0             0.000
----More (q=Quit, space/return=Continue)----
```

Variable definitions

The following table describes the parameters for the **show poe-power measurement** command.

Variable	Value
<portlist>	Enter the ports for which you want to display the power measurements. If you omit this parameter, the system displays all ports.

Display PoE Power Mode

Use the following procedure to display the PoE budget operating mode . There are 2 power budget modes; low (Fanless) or high (Normal).

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

```
PoE Main Status - Stand-alone
-------------------------------------------------
Power Mode                      : Low Power Budget
Available DTE Power             : 60 Watts
DTE Power Status                : Normal
DTE Power Consumption           : 0 Watts
DTE Power Usage Threshold       : 80 %
PD Detect Type                  : 802.3at and Legacy
Power Source Present            : AC Only
AC Power Status                 : Present
DC Power Status                 : Not Present
```

Enable or Disable PoE Traps

Enable or disable the traps for the PoE functions on the PWR+switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ```
   [no] snmp-server notification-control {pethPsePortOnOffNotification
   | pethMainPowerUsageOnNotification |
   pethMainPowerUsageOffNotification}
   ```

Variable definitions

The following table describes the parameters for the **snmp-server notification-control** command.

Variable	Value
pethPsePortOnOffNotification | pethMainPowerUsageOnNotification | pethMainPowerUsageOffNotification	Specifies a notification type
no	Disables the traps for the PoE function

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:

```
poe poe-limit [port <portlist>] <3-32>
```

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 PoE is enabled. **Note:** 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.

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:

Variable definitions

Use the data in the following table to use the **`poe poe-power-up-mode`** command.

Variable	Definition
802.3af	Sets the power up mode to normal.
802.3at	Sets the power up mode to 802.3at.
high-inrush	Sets power up mode to high inrush.

Table continues…

port <*LINE*>	Specify an individual port or list of ports.
pre-802.3at	Sets power up mode to pre-802.3at.

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 PoE is enabled. **Note:** If you omit this parameter, the system uses the port number you specified in the interface command.
{low | high | critical}	Specifies the PoE priority for the port.

Disable Port Power

About this task

Use this procedure to disable PoE 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:

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

3. Press Enter.

Configure PoE Power Mode using CLI

Use the steps in this section to configure the PoE power mode for the ERS3626GTS-PWR+ platform.

Important:

Only the ERS3626GTS-PWR+ operates in two PoE power modes - Fanless mode or Normal mode. The ERS3650GTS-PWR+ operates in Normal mode only.

- Fanless mode — Low Power Budget Mode (ERS3626GTS-PWR+ only)
- Normal mode — High Power Budget Mode (ERS3650GTS-PWR+ and ERS3626GTS-PWR+)

The default PoE power mode is Normal mode - High Power Budget Mode (fan operates).

In Normal mode the fans are always active, operating at different RPMs depending on sensor temperature. See Setting a power usage threshold on page 84. In Normal mode, the PoE budget is 740 Watts.

In Fanless mode (ERS3626GTS-PWR+ only), the fans operate at low RPM, thereby keeping the noise level low. To prevent the switch from overheating, the PoE budget is limited to 90 Watts. Although the internal temperature might show as High in this mode, the switch has been designed to operate at temperatures about 60°C. When the switch is operating in Fanless mode, diagnostic fan tests are not performed and the **`show environmental`** command does not display details about the fan.

Use the following procedure to set the PoE operating mode to low (Fanless) or high (Normal) power budget mode.

Important:

Only the ERS3626GTS-PWR+ operates in two PoE power modes - Fanless mode or Normal mode. The ERS3650GTS-PWR+ operates in Normal mode only.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [default] poe power-mode {low-power-budget| high-power-budget}
   ```

   Note:

   You do not need to reboot the switch for the change in power mode to take effect.

3. Verify the configuration.

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

Example

The following figure provides a sample output of the **show poe-main-status** command showing PoE power mode settings on the ERS3626GTS-PWR+ configured as Low Power Budget power mode.

```
Switch(config)#show poe-main-status
PoE Main Status - Stand-alone
-------------------------------------------------
Power Mode                  : Low Power Budget
Available DTE Power         : 90 Watts
DTE Power Status            : Normal
DTE Power Consumption       : 0 Watts
DTE Power Usage Threshold   : 80 %
PD Detect Type              : 802.3at
Power Source Present        : AC Only
AC Power Status             : Present
DC Power Status             : Not Present
```

The following figure provides a sample output of the **show poe-main-status** command showing PoE power mode settings on a switch configured as High Power Budget power mode (default).

```
Switch(config)#show poe-main-status
PoE Main Status - Stand-alone
-------------------------------------------------
Power Mode                  : High Power Budget
Available DTE Power         : 740 Watts
DTE Power Status            : Normal
DTE Power Consumption       : 0 Watts
DTE Power Usage Threshold   : 80 %
PD Detect Type              : 802.3at
Power Source Present        : AC Only
AC Power Status             : Present
DC Power Status             : Not Present
```

Variable definitions

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

Variable	Value
low-power-budget | high-power-budget	Specifies the power budget mode: • low-power-budget — for fanless mode **Note:** low-power-budget is supported on the ERS3626GTS-PWR+ platform only. • high-power-budget — for normal mode DEFAULT — high-power-budget (normal mode)
default	Resets the power mode to the default value — normal mode (high-power-budget)

View the PoE Module Firmware Version

About this task

Use this procedure to view the firmware version of the PoE module for all units in a stack.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command:

   ```
   show system {last-exception unit<1-8>|all} | verbose
   ```

Example

The following is an example output of the **`show system verbose`** command to view the PoE module firmware version of a stack unit.

The `PoE Module FW` field displays this information.

```
Switch:1# show system verbose
System Information:
        Operation Mode:       Stack, Unit # 3
        Size Of Stack:        3
        Base Unit:            1
        MAC Address:          C4-BE-D4-72-03-01
        PoE Module FW:        1.5.0.6
        Reset Count:          332
        Last Reset Type:      Software Download
        Autotopology:         Enabled
        Base Unit Selection:  Non-base unit using rear-panel switch
        sysDescr:             Ethernet Routing Switch 3650GTS-PWR+
                              HW:B2       FW:6.0.0.3   SW:v6.3.0.017
        sysObjectID:          1.3.6.1.4.1.45.3.83.4
        sysUpTime:            0 days, 00:18:45
        sysNtpTime:           NTP not synchronized.
        sysServices:          6
        sysContact:
        sysName:              3626GTS-PWR+
        sysLocation:
        Stack sysAssetId:
        Operational license:   Base Software
        Installed license:     Base Software
Unit #1 (Base Unit):
        Switch Model:         3650GTS-PWR+
        Pluggable Port 47:    (47) None
        Pluggable Port 48:    (48) None
        Pluggable Port 49:    (49) None
        Pluggable Port 50:    (50) SX
        Pluggable Port 51:    (51) Direct Attach Cable
        Pluggable Port 52:    (52) Direct Attach Cable
        MAC Address:          C4-BE-D4-72-03-00
        PoE Module FW:        1.5.0.11
        Hardware Version:     B2
        Firmware Version:     6.1.0.0
        Firmware FLASH:       6.0.0.3
        Software Version:     v6.3.0.017
        Software FLASH:       v6.3.0.017
        Serial Number:        16OL13600347
        Manufacturing Date:   20160405
        Fan #1 Status:        Normal
        Fan #2 Status:        Normal
        Fan #3 Status:        Normal
        Fan #4 Status:        Normal
        Unit sysAssetId:
Unit #2:
```

```
        Switch Model:          3650GTS-PWR+
        Pluggable Port 47:     (47) None
        Pluggable Port 48:     (48) None
        Pluggable Port 49:     (49) None
        Pluggable Port 50:     (50) SR
        Pluggable Port 51:     (51) Direct Attach Cable
        Pluggable Port 52:     (52) Direct Attach Cable
        MAC Address:           C4-BE-D4-72-0C-00
        PoE Module FW:         1.5.0.11
        Hardware Version:      B2
        Firmware Version:      6.1.0.0
        Firmware FLASH:        6.0.0.3
        Software Version:      v6.3.0.017
        Software FLASH:        v6.3.0.017
        Serial Number:         16OL13600356
        Manufacturing Date:    20160405
        Fan #1 Status:         Normal
        Fan #2 Status:         Normal
        Fan #3 Status:         Normal
        Fan #4 Status:         Normal
        Unit sysAssetId:
Unit #3:
        Switch Model:          3650GTS-PWR+
        Pluggable Port 47:     (47) None
        Pluggable Port 48:     (48) None
        Pluggable Port 49:     (49) None
        Pluggable Port 50:     (50) None
        Pluggable Port 51:     (51) Direct Attach Cable
        Pluggable Port 52:     (52) Direct Attach Cable
        MAC Address:           C4-BE-D4-72-02-00
        PoE Module FW:         1.5.0.6
        Hardware Version:      B2
        Firmware Version:      6.0.0.3
        Firmware FLASH:        6.0.0.3
        Software Version:      v6.3.0.017
        Software FLASH:        v6.3.0.017
        Serial Number:         16OL13600346
        Manufacturing Date:    20160405
        Fan #1 Status:         Normal
        Fan #2 Status:         Normal
        Fan #3 Status:         Normal
        Fan #4 Status:         Normal
        Unit sysAssetId:
```

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>
   ```

Variable definitions

Use the data in the following table to use the download **`sftp poe_module_image`** command.

Variable	Value
image_name	Specifies the image name.

Configuring IPv6 management using CLI

Enable IPv6 Globally

IPv6 administration is disabled by default.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   ipv6 enable
   ```

Enable IPv6 Interface on the Management VLAN

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <vlan ID>
   ```

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

   ```
   ipv6 interface enable
   ```

Display the IPv6 Interface Information

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 interface
   ```

Example

The following figure provides a sample of the **show ipv6 interface** command.

```
Switch#show ipv6 interface
================================================================================
                                    Interface Information
================================================================================
```

```
IFINDX VLAN-ID  MTU  PHYSICAL          ADMIN    OPER  RCHBLE  RETRAN  TYPE
                     ADDRESS           STATE    STATE TIME    TIME

-------------------------------------------------------------------------

=========================================================================
                                    Address Information
=========================================================================
INTF   IPV6                                    TYPE    ORIGIN    STATUS
INDEX  ADDRESS

-------------------------------------------------------------------------

0 out of 0 Total Num of Interface Entries displayed.

0 out of 0 Total Num of Address Entries displayed.
```

Display IPv6 Interface Addresses

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 address interface [<WORD>] [summary] [vlan <1-4094>]
   ```

Example

```
Switch#show ipv6 address interface
=============================================================================================
=========
                                    Address Information

=============================================================================================
========
IPV6                                                  VID/BID/ TYPE         ORIGIN
STATUS
ADDRESS                                          TID/LID
---------------------------------------------------------------------------------------------
--------
1::3                                                    V-1           UNICAST
MANUAL        PREF
3ffe:501:ffff:100:219:e1ff:fe4c:9400  V-1          UNICAST LINKLAYER    PREF
fe80::219:e1ff:fe4c:9400                     V-1          UNICAST LINKLAYER    PREF
=============================================================================================
=========
                                    Address Lifetime Information

=============================================================================================
========
IPV6                                                  VID/BID/     VALID
PREF
ADDRESS
   TID              LIFETIME       LIFETIME

---------------------------------------------------------------------------------------------
----------
1::3                                                    V-1
INF                  INF
3ffe:501:ffff:100:219:e1ff:fe4c:9400   V-1              2591990          604790
fe80::219:e1ff:fe4c:9400                     V-1              INF                INF
STATUS Legend:
```

```
PREF=PREFERRED, DEPR=DEPRECATED, INV=INVALID, INAC=INACCESSIBLE,
UNK=UNKNOWN TENT=TENTATIVE, DUP=DUPLICATE, INF=INFINITE
 3 out of 3 Total Num of Address Entries displayed.
```

Variable definitions

The following table describes the parameters for the **`show ipv6 address`** command.

Variable	Value
<WORD>	Specifies the IPv6 address. Length is 0 to 45.
summary	Displays IPv6 interfaces summary
vlan <1–4094>	Displays per vlan addresses for IPv6 interfaces

Configure IPv6 Interface Properties

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <vlan ID>
   ```

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

   ```
   ipv6 interface [address <ipv6_address/prefix_length>] [enable]
   [link-local <word>] [mtu {1280 - 9216}] [name <word>] [process-
   redirect] [reachable-time {0-3600000}] [retransmit-time {0-3600000}]
   ```

Variable definitions

The following table describes the parameters for the **`ipv6 interface`** command.

Variable	Value
address <*ipv6_address/prefix_length*>	Interface IPv6 address and mask prefix.
default ipv6 interface *[enable]*	Defaults all IPv6 interface parameters.
link-local <*WORD 0-19*>	Local link identifier. An alphanumeric value with a maximum of 19 characters.
mtu <*1280-9600*>	Default status: MTU 1500.
name <*1-255*>	Name: character string, from 1 to 255 in length.
reachable-time <*0-3600000*>	Time in milliseconds neighbor is considered reachable after a reachable confirmation message. Default: 30000.
retransmit-timer <*0-3600000*>	Time in milliseconds between retransmissions of neighbor solicitation messages to a neighbor. Default: 1000.

Display the Global IPv6 Configuration

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 global
   ```

Example

The following figure provides a sample of the **`show ipv6 global`** command.

```
Switch#show ipv6 global
forwarding                    : disabled
default-hop-cnt               : 30
number-of-interfaces          : 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
```

Configure an IPv6 Default Gateway

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable a default gateway, enter the following command:

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

3. To disable a default gateway, enter the following command:

   ```
   no ipv6 default-gateway
   ```

Display the IPv6 Default Gateway

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 default-gateway
   ```

Configure the IPv6 Neighbor Cache

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To add a static neighbor cache entry, enter the following command:

   ```
   ipv6 neighbor <ipv6_address> port <unit/port> mac <mac_addr>
   ```

3. To remove a static neighbor cache entry, enter the following command:

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

Display the IPv6 Neighbor Information

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 neighbor [<ipv6_address>] [type {other | dynamic | static
   | local}] [summary] [interface {loopback | tunnel | vlan}]
   ```

Example

The following figure provides a sample of the **`show ipv6 neighbor`** command.

```
Switch#show ipv6 neighbor

NET ADDRESS/           PHYS     TYPE    STATE
LAST
PHYSICAL ADDRESS       INTF   UPD
-------------------------------------------------------------------------------
2000::31/                      1/11   DYNAMIC REACHABLE  118
fc:a8:41:fb:c8:00
2000::40/                      V-1    LOCAL   REACHABLE  70
a0:51:c6:51:5c:00
2000::55/                      1/11   DYNAMIC STALE      121
1c:6f:65:a7:35:f6
fe80::1e6f:65ff:fea7:35f6/     1/11   DYNAMIC REACHABLE  102
1c:6f:65:a7:35:f6
fe80::a251:c6ff:fe51:5c00/     V-1    LOCAL   REACHABLE  70
a0:51:c6:51:5c:005

out of 5 Total Num of Neighbor Entries displayed.
```

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
```

Display IPv6 Interface Statistics

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 interface statistics
   ```

Example

The following figure provides a sample of the **`show ipv6 interface statistics`** command.

```
Switch#show ipv6 interface statistics
================================================================================
                                        Interface Stats
================================================================================

Icmp stats for IfIndex = 10001
IcmpInMsgs: 11
IcmpInErrors: 0
IcmpInDestUnreachs : 1
IcmpInAdminProhibs : 0
IcmpInTimeExcds : 0
IcmpInParmProblems : 0
IcmpInPktTooBigs : 0
IcmpInEchos : 1
IcmpInEchoReplies : 3
IcmpInRouterSolicits : 0
IcmpInRouterAdverts : 0
InNeighborSolicits : 3
InNbrAdverts : 3
IcmpInRedirects : 0
IcmpInGroupMembQueries : 0
IcmpInGroupMembResponses : 0
IcmpInGroupMembReductions : 0
IcmpOutMsgs : 22
IcmpOutErrors : 1
IcmpOutDestUnreachs : 0
IcmpOutAdminProhibs : 0
IcmpOutTimeExcds : 0
IcmpOutParmProblems : 0
IcmpOutPktTooBigs : 0
IcmpOutEchos : 4
IcmpOutEchoReplies : 1
IcmpOutRouterSolicits : 3
IcmpOutRouterAdvertisements : 0
IcmpOutNeighborSolicits : 8
IcmpOutNeighborAdvertisements : 5
IcmpOutRedirects : 0
IcmpOutGroupMembQueries : 0
IcmpOutGroupMembResponses : 7
IcmpOutGroupMembReductions : 0

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

Configure Stateless Address Auto-configuration

Use the following procedure to configure Global Stateless Address Auto-configuration (SLAAC).

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   ipv6 autoconfig
   ```

3. To view the SLAAC status, enter the following command:

   ```
   show ipv6 global
   ```

Example

The following figure provides a sample of the **show ipv6 global** command.

```
switch#show ipv6 global
forwarding                    : disabled
default-hop-cnt               : 30
number-of-interfaces          : 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                    : enabled
slow-path-to-cpu              : disabled
```

Configure IPv6 ICMP Port Unreachable

Use the following procedure to enable IPv6 ICMP port unreachable.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To configure IPv6, enter the following command:

   ```
   ipv6 enable
   ```

3. To enable ICMP Port Unreachable, enter the following command:

   ```
   ipv6 icmp port-unreach
   ```

4. To view the ICMP Port Unreachable status, enter the following command:

```
show ipv6 global
```

Example

The following figure provides a sample of the **show ipv6 global** command.

```
3549GTS-PWR+#show ipv6 global
forwarding                      : disabled
default-hop-cnt                 : 30
number-of-interfaces            : 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
```

Configure Processing Redirects on IPv6 Inband Interface

Use the following procedure to configure processing redirects on IPv6 inband interface.

Procedure

1. Enter Interface Configuration command mode:

   ```
   enable
   configure terminal
   interface vlan <vlan_ID>
   ```

2. To enable processing redirects, enter the following command:

   ```
   ipv6 interface process-redirect
   ```

3. To view processing redirect status for interface, enter the following command:

   ```
   show ipv6 interface process-redirect [vlan <vlan_ID>]
   ```

Example

The following figure provides a sample of the **show ipv6 interface process-redirect** command.

```
switch#show ipv6 interface process-redirect
================================================================================
                                      Process ICMP redirect status
================================================================================
Process ICMP redirect status for IfIndex = 10001
Enabled
```

Configure Neighbor Discovery Parameters

Use the following procedure to configure neighbor discovery parameters.

Procedure

1. Enter Interface Configuration command mode:

```
enable

configure terminal

interface vlan <vlan_ID>
```

2. To set the number of neighbor solicitation packets sent during duplicate address detection, enter the following command:

   ```
   ipv6 nd dad-ns <word>
   ```

3. To set the number of hops before packets are dropped, enter the following command:

   ```
   ipv6 nd hop-limit <word>
   ```

4. To view the neighbor discovery protocol information per interface, enter the following command:

   ```
   show ipv6 nd interface
   ```

Example

The following figure provides a sample of the **show ipv6 nd interface** command.

```
switch#show ipv6 nd interface
================================================================================
                         Interface Ipv6 Nd
================================================================================
INTF  VID/MID RTR-ADV MAX-INT MIN-INT LIFETIME HOP-LIM M-FLAG OTHER-CONF DAD-NS
INDEX TID/LID

--------------------------------------------------------------------------------
9001 L-1    False   600     200     1800     30      False  False      0
9003 L-3    False   600     200     1800     30      False  False      0
9004 L-4    False   600     200     1800     30      False  False      0
10001 V-1    True    600     200     1800     30      False  False      1

4 out of 4 Total Num of Ipv6 ND Entries displayed.
```

Display Neighbor Discovery Prefixes per Interface

Use the following procedure to view the neighbor discovery prefixes per interface.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To view the neighbor discovery prefixes per interface, enter the following command:

   ```
   show ipv6 nd-prefix interface
   ```

Example

The following figure provides a sample of the **show ipv6 nd-prefix interface** command.

```
switch#show ipv6 nd-prefix interface
================================================================================
                         Interface Ipv6 Nd Prefix
================================================================================
INTF  IPV6                                      VID/MID VALID    PREF     EUI
INDEX ADDRESS/PREFIX                            TID/LID LIFE     LIFE
```

```
--------------------------------------------------------------------------------
10001 8000::/64                                      1     2592000  604800   1
```

Enable the IPv6 Loopback Interface

Use the following procedure to enable the IPv6 loopback interface.

Note:

Only four IPv6 loopback interfaces can be configured.

Before you begin

Enable IPv6 globally.

Procedure

1. Log on to CLI in Loopback Interface Configuration mode:

   ```
   enable
   configure terminal
   interface loopback <1-16>
   ```

2. Enter the following command:

   ```
   [no] ipv6 interface [enable]
   ```

Variable definitions

The following table describes the parameters for the **ipv6 interface** command.

Variable	Value
no	Disables the IPv6 loopback interface.
enable	Enables the IPv6 loopback interface admin status.

Add Loopback Address to the Loopback Interface

Use the following procedure to add or delete the loopback address associated to the IPv6 loopback interface.

Before you begin

Enable IPv6 globally.

Procedure

1. Enter Loopback Interface Configuration mode:

   ```
   enable
   configure terminal
   interface loopback <1-16>
   ```

2. Enter the following command:

```
ipv6 interface address <address>
```

Display IPv6 Interface Loopback Information

Use the following procedure to display IPv6 interface loopback information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command:

   ```
   show ipv6 interface loopback <1-16>
   ```

Display IPv6 Neighbor Interface Loopback Information

Use this procedure to display IPv6 neighbor interface loopback information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 neighbor interface loopback <1-16>
   ```

Display IPv6 TCP Connections

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 tcp connections
   ```

Display IPv6 TCP Listeners

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipv6 tcp listener
   ```

Display IPv6 TCP Statistics

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show ipv6 tcp
```

Example

The following figure provides a sample of the **show ipv6 tcp** command.

```
Switch#show ipv6 tcp

show ipv6 tcp global statistics:
------------------
ActiveOpens:        0
PassiveOpens:       0
AttemptFails:       0
EstabResets:        0
CurrEstab:          0
InSegs:             0
OutSegs:            0
RetransSegs:        0
InErrs:             0
OutRsts:            0
HCInSegs:           0
HCOutSegs:          0
```

Display IPv6 UDP Statistics and Endpoints

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. To display UDP statistics, enter the following command:

```
show ipv6 udp
```

3. To display UDP endpoints, enter the following command:

```
show ipv6 udp endpoints
```

Defining 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.

The system retries connecting with the NTP server a maximum of 3 times, with 5 minutes between each retry. If the connection fails after the 3 attempts, the system waits for the next synchronization time (the default is 24 hours) and begins the process again.

Note:

The Power Source Present listing displays the current power source for the switch: AC Only.

Display SNTP Information

Display the SNTP information, as well as the configured NTP servers.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show sntp
   ```

Example

The following figure provides a sample output of the **`show sntp`** command.

```
switch#show sntp
SNTP Status:                   Disabled
Primary server address:         0.0.0.0
Secondary server address:       0.0.0.0
Sync interval:                  24 hours
Last sync source:               0.0.0.0
Primary server sync failures:   0
Secondary server sync failures: 0
Last sync time:                 Not Set
Next sync time:                 Not Set
Current time:                   Not Set
```

Enable or Disable SNTP

Enable or disable Simple Network Time Protocol . The default value for SNTP is Disabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. At the command prompt, enter the following command (without the optional *[no]* parameter to enable SNTP:

   ```
   [no] sntp enable
   ```

Variable definitions

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

Variable	Value
no	Disables SNTP

Set SNTP Server Primary Secondary Address

Set or clear the IP address for the primary or secondary NTP server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] sntp server <primary|secondary> address <A.B.C.D>
   ```

Variable definitions

The following table describes the parameters for the **`sntp server <primary|secondary> address`** command.

Variable	Value
<A.B.C.D>	Enter the IP address of the primary or secondary NTP server in the format XXX.XXX.XXX.XXX. DEFAULT: 0.0.0.0.
no	Clears the NTP server IP addresses
<primary|secondary>	Enter the NTP server you want to set or clear: • primary — the IP address for the primary NTP server • secondary — the IP address for the secondary NTP server

Force a Manual Synchronization with NTP Server

Force a manual synchronization with the NTP Server. This procedure is useful if the recurring synchronization is long, and you want to correct or test the operation immediately, rather than waiting for, or changing the reoccurrence period.

Before you begin

You must enable SNTP before this procedure can be performed.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   sntp sync-now
   ```

Set up Recurring Synchronization

You can specify recurring synchronization with the NTP server in hours, relative to the 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>
   ```

Variable definitions

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

Variable	Value
<0–168>	Specifies the number of hours you want for periodic synchronization with the NTP server. • 0– synchronization at start-time only • 168 — once a week DEFAULT: 24 hours

Set SNTP Parameters to Default

Setting the SNTP parameters to their default values allows you to disable SNTP, clear stored SNTP server addresses, and restore the default SNTP synchronization interval.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   default sntp [enable | server | sync-interval]
   ```

Enable or Disable UTC Timestamp

Use this procedure to enable or disable the display of the UTC timestamp. 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
```

Testing Cable Diagnostic

Use this procedure to run a cable diagnostic test globally, or for one or more specific switch ports.

Test Cables with TDR using CLI

About this task

Use this procedure to run a cable diagnostic test 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:

```
tdr test <portlist>
```

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 using CLI

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>
```

Variable definitions

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

Variable	Definition
<portlist>	Specifies a port or list of ports.

Using Domain Name Server

You can use the Domain Name Server (DNS) client to ping or Telnet to a host server or to a host by name.

To use this feature, you must configure at least one DNS. You can also configure a default domain name. If you configure a default domain name, that name is appended to host names that do not contain a dot. The default domain name and addresses are saved in NVRAM.

The host names for ping and Telnet cannot be longer than 63 alphanumeric characters, and the default DNS domain name cannot be longer than 255 characters.

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

Display the DNS Domain Name

Display the DNS domain name, as well as any configured servers.

Procedure

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

   ```
   show ip dns
   ```

Example

The following figure provides a sample of the **show ip dns** command.

```
switch>show ip dns
DNS Default Domain name: None

DNS Servers
------------
0.0.0.0
0.0.0.0
0.0.0.0
```

Ping the Host

You can test the network connection to another network device using the **ping** command. The command sends an Internet Control Message Protocol (ICMP) packet from the switch to the target device.

You can ping a host using either its IP address or hostname.

Before you begin

A local IP address must be set before issuing the **ping** command.

Procedure

1. To enter User EXEC mode, log on to the switch.

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

```
ping <A.B.C.D or Hostname>
```

Variable definitions

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

Variable	Value
<A.B.C.D or Hostname>	Specifies: • the IP address of the target device in dotted-decimal notation (A.B.C.D in the format XXX.XXX.XXX.XXX) • the hostname of the device to ping. The hostname can be a simple name, such as fred; in this case the DNS domain name, if set, is appended. Or the hostname can be a full hostname, such as fred.ca.extremenetworks.com. DEFAULT: none

Configure the IP Address of a DNS Server

Add or remove one or more DNS servers' IP addresses. You can add or remove up to three servers; one at a time.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
[no] ip name-server <A.B.C.D>
```

Variable definitions

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

Variable	Value
<A.B.C.D>	Specifies the IP address of a DNS server to be added or removed in the format XXX.XXX.XXX.XXX. DEFAULT: 0.0.0.0
no	Removes the specified DNS server name.

Set the Systems DNS Domain Name

Specifies the 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] [default] ip domain-name [<LINE>]
   ```

Variable definitions

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

Variable	Value
<LINE>	Specifies the system's DNS domain name. DEFAULT: empty string
no	Clears the system's DNS domain name (sets it to an empty string).
default	Clears the system's DNS domain name (sets it to an empty string).

Saving Automatically

By default, every 60 seconds the switch checks whether a configuration change occur, or if a log message is written to nonvolatile storage. If one of these two events has occurred, the system automatically saves its configuration and the nonvolatile log to flash memory. Also, the system automatically saves the configuration file if a system reset command is invoked by the user.

Important:

Do not power off the switch within 60 seconds of changing configuration parameters. Doing so causes loss of changes in the configuration parameters.

You can enable or disable the autosave feature using the **autosave enable** and **no autosave enable** commands.

You can use CLI command **copy config nvram** to force a manual save of the configuration when the autosave feature is disabled.

Display Autosave Status

Display the status of the autosave feature, either enabled or disabled.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

```
show autosave
```

Example

The following figure provides a sample of the **show autosave** command.

```
switch#show autosave
Auto Save: Enabled
```

Configure Autosave

The switch performs a check every 60 seconds to detect changes to the configuration file or a new log message in the nonvolatile storage. If any of these events occurs, the switch automatically saves its configuration and the nonvolatile log to flash memory. Autosave also automatically saves your configuration information following restarts.

You can enable or disable the Autosave feature. After you disable autosave, changes in the configuration file are not saved to the flash memory.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] [default] autosave enable
   ```

Variable definitions

The following table describes the parameters for the **autosave enable**command.

Variable	Value
no	Disables the autosave feature.
default	Returns the autosave feature to the default value. DEFAULT: Autosave Enabled

Display CLI Settings

Display the current CLI settings, such as general console settings, mode, user names and passwords, and password types.

Procedure

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

   ```
   show cli {info | list | mode | password [type | unit <1-8>]}
   ```

Example

The following figure provides a sample of the **show cli** command.

```
switch>show cli info
Inactivity Timeout:  15 minute(s)
Login Timeout: 1 minute(s)
Login Retries: 3
More: True
Screen Lines: 23
```

Variable definitions

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

Variable	Value
info	Displays general Console settings
list	Lists CLI tree
mode	Displays information about current CLI mode
password [type]	Displays the current password type configured for serial console and Telnet access to the stack, or standalone switch. Values include: • local — the system local password is used • none — no password is used • radius — RADIUS password authentication is used • tacacs — TACACS+ AAA services are used
password [unit <1–8>]	Displays current CLI user names and passwords for a specific unit or all units.

Displaying interfaces

You can view the status of all interfaces on the switch, including MultiLink Trunk membership, link status, autonegotiation, and speed.

Display Interfaces

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

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

Procedure

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

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

Example

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

```
switch>show interfaces names 1,2,3
Port   Name
----   ----
1      LabBldg
2      Testing
3      FloorBldg
```

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

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

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

```
switch>show interfaces verbose
Port:    1
     Trunk:
     Admin Status: Enable
     Oper Status:  Up
     EAP Oper Status: Up
     VLACP Oper Status:  Down
     STP Oper Status:  Forwarding
     Link: Up
     LinkTrap: Enabled
     Link Autonegotiation:  Custom
     Link Speed:  1000Mbps
     Link Duplex:  Full=Duplex
     BPDU-guard (BPDU Filtering): Disabled
     BPDU-guard (BPDU Filtering): Oper Status: N/A
Port:    2
     Trunk:
     Admin Status: Enable
     Oper Status:  Down
     EAP Oper Status: Up
     VLACP Oper Status:  Down
     STP Oper Status:  Discarding
     Link: Down
     LinkTrap: Enabled
     Link Autonegotiation:  Custom
     BPDU-guard (BPDU Filtering): Disabled
     BPDU-guard (BPDU Filtering): Oper Status: N/A
----More (q=Quit, space/return=Continue)----
```

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

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

Variable definitions

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

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

Display Interface Configurations

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

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

Procedure

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

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

Example

The following figure provides a sample of the **show interfaces config** command.

```
switch>show interfaces 1/1 config
Unit/Port:    1/1
     Trunk:
     Admin Status: Enable
     Oper Status:  Up
     EAP Oper Status: Up
     VLACP Oper Status:  Down
     STP Oper Status:  Forwarding
     Link: Up
     LinkTrap: Enabled
     Link Autonegotiation:  Enabled
```

```
     Link Speed:  100Mbps
     Link Duplex:  Full-Duplex
     Flow Control:  Disable
     BPDU-guard (BPDU Filtering): Disabled
     BPDU-guard (BPDU Filtering): Oper Status: N/A

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

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

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

Variable definitions

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

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

Configure the Asset ID

Configure the Asset ID of a switch or stack to identify the switch using your company-specific inventory or asset tracking information.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] [default] asset-id [stack | unit <1-8>] <WORD>
   ```

3. Verify the Asset ID using one of the following commands:

   ```
   show system
   ```

   OR

   ```
   show tech
   ```

   OR

   ```
   show sys-info
   ```

OR

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

Variable definitions

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

Variable	Value
stack	Configures the Asset ID of a stack.
unit <*1–8*>	Configures the Asset ID of a specific unit. Enter unit number 1–8.
WORD	Specifies the Asset ID which corresponds to your asset tracking system. Enter an alphanumeric Asset ID of up to 32 characters.
no	Removes the Asset ID of a specific unit. Enter a unit number 1–8.
default	Returns the Asset ID of a specific unit to the default value. Enter a unit number 1–8.

Configuring Energy Saver using CLI

You can use Energy Saver to configure the switch to utilize energy more efficiently.

Configure Global Energy Saver

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure global Energy Saver:

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

Variable definitions

The following table defines optional parameters that you can enter with the **[no] [default] energy-saver [enable] [efficiency-mode] [poe-power-saving]** command.

Variable	Value
[default]	Configures Energy Saver efficiency mode, POE power saving, or global Energy Saver to default values (disabled).
efficiency-mode	Enables Energy Saver efficiency mode. **Important:** You must ensure that SNTP is enabled before you can enable Energy Saver efficiency mode. **Important:** You must disable Energy Saver globally before you can modify Energy Saver efficiency mode. **Important:** 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.
enable	Enables Energy Saver globally.
[no]	Disables Energy Saver efficiency mode, POE power saving, or Energy Saver globally.
poe-power-saving	Enables POE power saving. **Important:** You must disable Energy Saver globally before you can modify POE power saving.

Configure Port-based Energy Saver

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

Before you begin

- Disable Energy Saver globally.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet
   ```

2. Configure port-based Energy Saver.

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

Variable definitions

The following table defines optional parameters that you can enter with the **`[no] [default] energy-saver <enable> [port <portlist> enable]`** command.

Variable	Value
default	Configures Energy Saver to default value (disabled).
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

Use the following procedure to have Energy Saver enabled, but not activated.

Before you begin

- Disable Energy Saver globally.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Activate Energy Saver.

   ```
   energy-saver activate
   ```

3. Deactivate Energy Saver.

   ```
   energy-saver deactivate
   ```

Configure Energy Saver Schedule

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.

Before you begin

- Disable Energy Saver globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure Energy Saver scheduling.

   ```
   energy-saver schedule {weekday|weekend|monday|tuesday | wednesday|
   thursday|friday|saturday|sunday} <hh:mm> {activate|deactivate}
   ```

Variable definitions

The following table defines parameters that you can enter with the **energy-saver schedule {weekday|weekend|monday|tuesday |wednesday|thursday|friday|saturday|sunday} <hh:mm> {activate|deactivate}** command.

Variable	Value
<activate>	Specifies the 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 Schedule

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

Before you begin

- Disable Energy Saver globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable Energy Saver scheduling.

   ```
   no energy-saver schedule
   ```

Variable definitions

The following table defines optional parameters that you can enter after the **no energy-saver schedule** command.

Variable	Value
monday|tuesday|wednesday |thursday|friday| saturday|sunday	Disables Energy Saver scheduling for a specific day.
<hh:mm>	Specifies the scheduled time to disable Energy Saver (hour and minutes).
weekday	Disables Energy Saver scheduling for all weekdays.

Table continues…

Variable	Value
weekend	Disables Energy Saver scheduling for Saturday and Sunday.

Configure Energy Saver Scheduling to default

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

Before you begin

- Disable Energy Saver globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure Energy Saver scheduling.

   ```
   default energy-saver schedule
   ```

Variable definitions

The following table defines optional parameters that you can enter after the **`default energy-saver schedule`** command.

Variable	Value
friday|monday|saturday|sunday|thursday|tuesday|wednesday	Configures 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 Schedule

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

Procedure

1. To enter User EXEC mode, log on to the switch.
2. View Energy Saver schedule.

   ```
   show energy-saver schedule
   ```

Example

The following example displays sample output for the **show energy-saver schedule** command.

```
switch> show energy-saver schedule
Day            Time        Action
---            ----        ------
Monday         08:00        Activate
Wednesday     11:00        Activate
Friday         14:00        Activate
```

View Energy Saver Energy Saving

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

Procedure

1. To enter User EXEC mode, log on to the switch.
2. View Energy Saver savings.

   ```
   show energy-saver savings
   ```

   Important:

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

Example

The following example displays sample output for the **show energy-saver savings** command.

```
Switch> show energy-saver savings
Unit #        Model            Switch Capacity Saving        PoE Saving
------        -----            ----------------------        ----------
1            3524GT-PWR        0.0 watts                        0.0 watts
-------------------------------------------------------------------
TOTAL                            0.0 watts                        0.0 watts
===================================================================
```

View the Global Energy Saver Configuration

Use the following procedure to review the Energy Saver configuration for the switch.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. View the global Energy Saver configuration

   ```
   show energy-saver
   ```

Example

The following example displays sample output for the **show energy-saver** command.

```
Switch> show energy-saver
Extreme Networks Energy Saver:        Enabled
Extreme Networks Energy Saver PoE Power Saving Mode:             Enabled
Extreme Networks Energy Saver Efficiency-Mode Mode:             Disabled
Day/Time:                                    Thursday 13:33:53
Current Extreme Networks Energy Saver state:                         Energy Saver is
Inactive
```

View the Port-based Energy Saver Configuration

Use the following procedure to review Energy Saver configuration for all ports on the switch, an individual port, or range of ports.

Procedure

1. To enter User EXEC mode, log on to the switch.
2. View Energy Saver savings.

   ```
   show energy-saver interface <portlist>
   ```

Example

The following example displays sample output for the **show energy-saver interface** command using the *<portlist>* variable.

```
switch> show energy-saver interface 1-6
Port        Energy Saver     PoE Savings        PoE Priority
----        ---------        -----------        ------------
1            Enabled             N/A                 N/A
2            Enabled             N/A                 N/A
3            Disabled          N/A                  N/A
4            Enabled             N/A                 N/A
5            Enabled             N/A                 N/A
6            Disabled          N/A                  N/A
```

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. Enter the following command:

   ```
   show flash history [unit <1 - 8 >]
   ```

Note:

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

Example

The following is an example for a single unit.

```
--------------------------------------------------------------------------------
FLASH Write History Unit:
--------------------------------------------------------------------------------
Section                 Number of writes
--------------------------------------------------------------------------------
Diagnostics Image:         2
Agent Image:               14
Config Area:               471
Auxiliary Config Area:     469
CRC Block :                472
--------------------------------------------------------------------------------
* Number of minimum guaranteed writes: 100 000
--------------------------------------------------------------------------------
```

The following is an example for stacked units.

```
--------------------------------------------------------------------------------
FLASH Write History Unit 1:
--------------------------------------------------------------------------------
Section                 Number of writes
--------------------------------------------------------------------------------
Diagnostics Image:         0
Agent Image:               3
Config Area:               22
Auxiliary Config Area:     22
CRC Block :                22
--------------------------------------------------------------------------------
* Number of minimum guaranteed writes: 100 000
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
FLASH Write History Unit 2:
--------------------------------------------------------------------------------
Section                 Number of writes
--------------------------------------------------------------------------------
Diagnostics Image:         0
Agent Image:               3
Config Area:               21
Auxiliary Config Area:     21
CRC Block :                21
--------------------------------------------------------------------------------
* Number of minimum guaranteed writes: 100 000
--------------------------------------------------------------------------------
```

Variable definitions

The following table describes the parameters for the show flash history command.

Variable definition

Variable	Value
unit <1 –8 >	Provides information from the specified unit 1 to 8. If no unit is specified, the number of writes for all stacked units displays.

Run the VS script

About this task

The script deletes previously configured settings, such as VS VLAN.

Before you begin

The switch is in the factory default state.

Procedure

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

   ```
   run vs
   ```

3. Press **Enter**.

Example

```
#run vs
************************************************************
This script will guide you through configuring the ***
Extreme Networks switch for optimal operation with VideoSurveillance.***
------------------------------------------------- ***
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. ***
************************************************************
Video Surveillance VLAN ID [45] :
VS Camera Ports (stack/port,stack/port...):1-20
VS Camera port speed (1 = tri-speed, 2 = dual-speed) [1]:
Is the VS Uplink going to be a Trunk/MLT? y/n [y]:
VS Uplink MLT ID (1-6) [1]:
VS Uplink MLT ports (stack/port,stack/port):25-26
Do you want to enable IP routing? y/n [n]:y
VS VLAN IP Address [192.0.2.1] :
VS VLAN Subnet Mask [255.255.255.0] :
Do you want to enable the DHCP server? y/n [n]:y
VS scope start IP address[192.0.2.2]:
VS scope end IP address[192.0.2.3]:
VS scope netmask[255.255.255.0]:

% The Video Surveillance VLAN ID has been set to 45
% Ports for Video Surveillance [1-20] have been set
% Ports [1-20] have been removed from management vlan
% Pvid for ports [1-20] has been set to 45
% Tagging for ports [1-20] has been set to unTagAll
% MLT Id [1] has been set
% MLT ports [25-26] have been set
% The VS VLAN IP address has been set to 192.0.2.1
% The VS VLAN IP network mask has been set to 255.255.255.0
% The VS scope IP start address has been set to 192..0.2.2
% The VS scope IP end address has been set to 192.0.2.3
% The VS scope IP network mask has been set to 255.255.255.0
```

The settings from this script can be displayed by using the CLI command `show running-config`.

Display System Information

Display the current system characteristics.

Important:

You must enable and configure SNTP to display GMT time. Refer to Simple Network Time Protocol (SNTP) on page 106 for more details.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show sys-info
   ```

Example

The following example provides a sample output of the **`show sys-info`** command.

```
Switch>show sys-info
Operation Mode:         Stack, Unit # 1
Size Of Stack:          2
Base Unit:              1
MAC Address:            C4-BE-D4-72-27-01
PoE Module FW:          1.5.0.6
Reset Count:            150
Last Reset Type:        Software Download
Autotopology:           Enabled
Pluggable Port 23:      None
Pluggable Port 24:      SX
Pluggable Port 25:      None
Pluggable Port 26:      None
Pluggable Port 27:      Unsupported
Pluggable Port 28:      Unsupported
Base Unit Selection:    Base unit using rear-panel switch
sysDescr:               Ethernet Routing Switch 3626GTS-PWR+
                        HW:B2       FW:6.0.0.3    SW:v6.1.0.043
                        Mfg Date:20160405    HW Dev:none
Serial #:               16OL14300004
Operational Software:   FW:6.0.0.3    SW:v6.1.0.043
Installed software:     FW:6.0.0.3    SW:v6.1.0.043
Operational license:    Base software
Installed license:      Base software
sysObjectID:            1.3.6.1.4.1.45.3.83.2
sysUpTime:              10 days, 01:43:23
sysNtpTime:             NTP not synchronized.
sysServices:            6
sysContact:
sysName:                Lord_1.4
sysLocation:
Stack sysAssetId:
Unit sysAssetId:
```

Configuring the switch using EDM

Configure Remote Access using EDM

Use this procedure to configure remote access for a switch.

Procedure

1. In the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Remote Access**.
3. In the work area, click the **Setting** tab.
4. In the Telnet Remote Access Setting section, select a value from the **Access** list.
5. In the Telnet Remote Access Setting section, select a value from the **Use List** list.
6. In the SNMP Remote Access Setting section, select a value from the **Access** list.
7. In the SNMP Remote Access Setting section, select a value from the **Use List** list.
8. In the Web Page Remote Access Setting section, select a value from the **Use List** list.
9. In the SSH Remote Access Setting section, select a value from the **Access** list.
10. In the SSH Remote Access Setting section, select a value from the **Use List** list.
11. On the toolbar, click **Apply**.

Remote Access Setting Tab Field Descriptions

Use the data in the following table to use the **Remote Access Setting** tab.

Name	Description
Telnet Remote Access Setting	Specifies the remote access settings for telnet sessions: • **Access**: Allows or disallows telnet access to the switch • **Use List** : Enables (Yes) or disables (No) the use of listed remote Telnet information.
SNMP Remote Access Setting	Specifies SNMP remote access settings: • **Access**: Allows or disallows SNMP access to the switch • **Use List** : Enables (Yes) or disables (No) the use of listed remote SNMP information.

Table continues…

Name	Description
Web Page Remote Access Setting	Specifies web page remote access settings: • **Use List**: Enables (Yes) or disables (No) the use of listed remote web page information.
SSH Remote Access Setting	Specifies SSH access settings: • **Access**: Allows or disallows SSH access to the switch • **Use List** : Enables (Yes) or disables (No) the use of listed remote SSH information.

Configure IP Office Script using EDM

Use the following procedure to configure IP Office in default or 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, double-click **Run Scripts**.

   The **IP Office Script** work area displays.
3. 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.
4. In the Verbose work area, type the Voice VLAN ID in the **Voice VLAN Id** dialog box.
5. In the **Voice VLAN Gateway** dialog box, type the VLAN IP address.
6. In the **Voice VLAN Gateway Mask** dialog box, enter the VLAN IP mask address.
7. In the **Data VLAN Id** dialog box, type the data VLAN ID.
8. In the **Data VLAN Gateway** dialog box, type the data VLAN Gateway IP address.
9. In the **Data VLAN Gateway Mask** dialog box, type the data VLAN Gateway IP mask address.
10. In the **IP Route to Gateway Modem-Router** dialog box, type the IP route address of the Gateway Modem-Router.
11. In the **IP Office Call-Server** dialog box, type the call server IP address.

12. In the **IP Office File-Server** dialog box, type the file server IP address.
13. Click **Apply**.

IP Office Script Tab Field Descriptions

Use the data in the following table to use the **IP Office script** tab.

Name	Description
Run Script Mode	Specifies to run the script either in default or verbose mode.
Voice VLAN ID	Specifies the voice VLAN ID. By default, the voice VLAN ID is 42.
Voice VLAN Gateway	Specifies the Voice VLAN Gateway IP Address. By default, the voice VLAN gateway IP address is 192.168.42.254
Voice VLAN Gateway Mask	Specifies the voice VLAN gateway IP mask address. By default, the voice VLAN gateway IP mask address is 255.255.255.0 The default subnet mask created by the run IP Office script supports a maximum of 250 hosts. You can change the subnet mask to 255.255.254.0 to allow 510 hosts for each subnet using the verbose mode.
Data VLAN ID	Specifies the data VLAN ID. By default, the data VLAN ID is 44.
Data VLAN Gateway	Specifies the data VLAN Gateway. By default, the data VLAN Gateway is 192.168.44.254
Data VLAN Gateway Mask	Specifies the data VLAN Gateway Mask. By default, the data VLAN Gateway Mask is 255.255.255.0
IP Route to Gateway Modem-Router	Specifies the IP Route to gateway modem and router. By default, the IP address is 192.168.44.2
IP Office Call-Server	Specifies the IP Office call server IP address. By default, the call server IP address is 192.168.42.1
IP Office File-Server	Specifies the IP Office file server IP address. By default, the file server IP address is 192.168.42.1
Status	Displays the status of the last action that occurred since the switch last booted. Values include: • other—no action occurred since the last boot. • inProgress—the selected operation is in progress. • passed—the selected operation succeeded. • failed—the selected operation failed.

View Switch Information using EDM

Use this procedure to display switch specific information such as the type of switch, hardware version number, serial number, the number of base ports, and the total number of ports.

Procedure

1. From the Device Physical View, click a switch.
2. From the navigation tree, click **Edit**.
3. In the Edit tree, click **Unit**.

Unit Tab Field Descriptions

Use the data in the following table to use the **Unit** tab.

Name	Description
Type	Specifies the type of switch.
Descr	Description of switch.
Ver	Specifies the hardware revision number of the switch.
SerNum	Specifies the serial number of the switch.
BaseNumPorts	Specifies the base number of ports.
TotalNumPorts	Specifies the total number of ports.

Configure Interface Ports

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

Before you begin

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

About this task

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

Procedure

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

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

Field Descriptions

The following table describes configuring interface ports.

Name	Description
Index	Indicates a unique value assigned to each interface port.
Name	Specifies a name for the port.
Descr	Indicates the description for the port.
Type	Indicates the media type for the port.
Mtu	Indicates the size of the largest packet that can be sent or received, in octets.
PhysAddress	Indicates the MAC address assigned to the port.
AdminStatus	Specifies the current administrative state of the port. Values include: • up • down All ports start in an up state on a managed system. The AdminStatus changes do down due to administrator action or the configuration information.
OperStatus	Indicates the current operational state of the port. Values include: • up — port is ready to transmit and receive traffic • down — port is not ready to transmit and receive traffic

Table continues…

Name	Description
	• testing — port is currently being tested
LastChange	Indicates the value of sysUpTime at the time the interface entered into the current state. If the current state occurred before the last reinitialization of the local management subsystem, the value is zero.
LinkTrap	Specifies if traps are generated for this port.
AutoNegotiate	Specifies if Autonegotiation is enabled or disabled on the port.
AdminDuplex	Specifies the duplex mode of the port. Values include: • half • full
OperDuplex	Indicates the current duplex mode of the port.
AdminSpeed	Specifies the speed of the port. Values include: • mbps10 • mbps100 • mbps1000 • mbps10000
OperSpeed	Indicates the current speed of the port.
FlowControlAdminMode	Specifies the flow control mode of the port. Values include: • disabled — flow control disabled • enabledXmit — transmit enabled • enabledRcv — receive enabled • enabledXmitAndRcv — transmit and receive enabled
FlowControlOperMode	Indicated the current flow control mode of the port.
AutoNegotiationCapability	Indicates the current auto negotiation capability of the port.
AutoNegotiationAdvertisements	Specifies the custom auto negotiation advertisements of the port Values include: • 10Half • 10Full • 100Half • 100Full • 1000Half • 1000Full

Table continues…

Name	Description
	• 10000Full • PauseFrame • AsymmPauseFrame
MltId	Indicates the MultiLink Trunk assigned to the port.
IsPortShared	Indicates whether the port is shared.
PortActiveComponent	Indicates the port components active for a shared port.

Configure System Parameters using EDM

Use this procedure to view and modify the system level configuration.

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, click the **System** tab.
5. In the **sysContact** dialog box, type system contact information.
6. In the **sysName** dialog box, type a system name.
7. In the **sysLocation** field, type a system location.
8. Perform one of the following:
   - To enable authentication traps, select the **Authentication Traps** check box.
   - To disable authentication traps, clear the **Authentication Traps** check box.
9. In the **Reboot** section, click a radio button.
10. In the **AutoPvid** section, click a radio button.
11. In the **BootMode** section, click a radio button.
12. On the toolbar, click **Apply**.

System Tab Field Descriptions

Use the data in the following table to use the **System** tab.

Name	Description
sysDescr	Provides device specific information. This is a read-only item.

Table continues…

Name	Description
sysUpTime	Indicates the amount of time since the system was last booted.
sysObjectID	Indicates the system object identification number. This is a read-only field.
sysContact	Specifies contact information for the system administrator, which can include a contact name or email address.
sysName	Specifies a unique name to describe this switch.
sysLocation	Specifies the physical location of this device.
SerNum	Indicates the serial number of this switch.
AuthenticationTraps	Enables or disables authentication traps. When enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When disabled, no SNMP traps are received.
Reboot	Options include: • **running**: the switch remains in the running mode (default) • **reboot** : initiates a hardware reset.
AutoPVID	When enabled, a VLAN ID can be automatically assigned to any port.
NextBootMgmtProtocol	Indicates the transport protocols to use after the next switch restart. This is a read-only item.
CurrentMgmtProtocol	Indicates the current transport protocols that the switch supports. This is a read-only item.
BootMode	Specifies whether to use the BootP or DHCP server to assign an IPv4 address for the management VLAN at the next switch reboot. Values include: • **other**: read only • **bootpDisabled**: use configured server IP address • **bootpAlways**: always use the BootP server • **bootpWhenNeeded**: use the BootP server when necessary • **bootpOrLastAddress**: use the BootP server last used • **dhcpAlways**: always use the DHCP server • **dhcpWhenNeeded**: use the DHCP server when necessary • **dhcpOrLastAddress**: use the DHCP server last used

Table continues…

Name	Description
ImageLoadMode	Indicates the source from which to load the agent image at the next boot. This is a read-only items.
CurrentImageVersion	Indicates the version number of the agent image that is currently used on the switch. This is a read-only item.
LocalStorageImageVersion	Indicates the version number of the agent image that is stored in flash memory on the switch. This is a read-only item.
NextBootDefaultGateway	Indicates the IP address of the default gateway for the agent to use after the next time you boot the switch. This is a read-only item.
CurrentDefaultGateway	Indicates the address of the default gateway that is currently in use. This is a read-only item.
NextBootLoadProtocol	Indicates the transport protocol that the agent uses to load the configuration information and the image at the next boot. This is a read-only item.
LastLoadProtocol	Indicates the transport protocol last used to load the image and configuration information about the switch. This is a read-only item.

Configure the Asset ID using EDM

Use this procedure to configure the Asset ID for a switch or stack.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, click the **Asset ID** tab.
5. In the table, click the cell under the **Asset ID** column heading.
6. In the **Asset ID** field, enter an alphanumeric value, up to 32 characters.
7. On the toolbar, click **Apply**.

Select the CLI Banner Type using EDM

Use this procedure to select the type of banner that is displayed in the Command Line (CLI) Telnet screen.

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, select the **Banner** tab.

Banner Tab Field Descriptions

Use the data in the following table to use the **Banner** tab.

Name	Description
BannerControl	Specifies the banner to be displayed when you connect to a switch device using Telnet. Values include: • **static**: uses a predefined static banner. • **custom**: uses a custom banner. • **disabled** : prevents the display of any banner.

Customize CLI Banner using EDM

Use this procedure to customize the banner that is displayed in the Command Line (CLI) Telnet screen. A customer banner is 19 lines high and can be up to 80 characters long.

Before you begin

Select **custom** for the CLI banner type.

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, select the **Custom Banner** tab.
5. To select a switch for which to customize the banner, click a row.
6. In the row, double-click the cell in the **Line** column.
7. Type a character string for the banner.
8. On the toolbar, click **Apply**.

Custom Banner Tab Field Descriptions

Use the data in the following table to use the **Custom Banner** tab.

Name	Description
Type	Indicates whether the banner type is for a standalone (switch) or a stack (stack).
Id	Indicates the line of text within a custom banner.
Line	Specifies the banner character string. The custom banner is 19 lines high and can be up to 80 characters long.

Configure AUR

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

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, select the **AUR** tab.
5. To enable Auto Unit Replacement, select the **AutoUnitReplacementEnabled** check box.
6. To enable Auto Unit Replacement saving, select the **AutoUnitReplacementSaveEnabled** check box.
7. Enter a value for forced saves in the **AutoUnitReplacementForceSaves** field.
8. Enter a value for AUR restore in the **AutoUnitReplacementRestore** field.
9. Click **Apply**.

AUR Tab Field Descriptions

Use the data in the following table to use the **AUR** tab.

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

Change Switch Software using EDM

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

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **File System**.
3. On the work area, click the **Config/Image/Diag file** tab.
4. In the **TftpServerInetAddressType** section, click a radio button.
5. In the **TftpServerInetAddress** dialog box, type the TFTP server IP address.
6. In the **BinaryConfigFileName** dialog box, type the name of the binary configuration file.
7. In the **ImageFileName** dialog box, type the name of the current image file.
8. In the **FwFileName(Diagnostics)** dialog box, type the name of the current diagnostic file.
9. In the **Action** section, click a radio button.
10. On the toolbar, click **Apply**.

Config/Image/Diag File Tab Field Descriptions

Use the data in the following table to use the **Config/Image/Diag File** tab.

Name	Description
TftpServerInetAddressType	Specifies the type of TFTP address: • **IPv4** • **IPv6**
TftpServerInetAddress	Specifies the IP address of the TFTP server on which the new software images are stored for download.
BinaryConfigFileName	Specifies the binary configuration file currently associated with the switch.
ImageFileName	Specifies the name of the image file currently associated with the switch. You can change this value to the name of the software image to be downloaded.
FwFileName(Diagnostics)	Specifies the name of the diagnostic file currently associated with the switch. You can change this field to the name of the diagnostic software image to be downloaded.

Table continues…

Name	Description
Action	Specifies the actions taken during this file system operation. The available options are: • **other** • **dnldConfig**: downloads a configuration file to the switch. The new configuration file is implemented on the next switch boot cycle. • **upldConfig**: uploads a configuration file to a server from the switch. The configuration file contains the current switch MIB object value. • **dnldImg**: downloads a new software image to the switch. • **dnldImgIfNewer**: downloads a new software image to the switch only if it is newer than the image currently saved on FLASH. • **dnldImgNoReset**: downloads a new software image to the switch, but does not reset the switch when the download is complete. • **dnldFw**: downloads new firmware to the switch. • **dnldFwNoReset**: downloads new firmware to the switch, but does not reset the switch when the download is complete.
Status	Displays the status of the last action that occurred since the switch last booted. Values include: • **other**: no action occurred since the last boot. • **inProgress**: the selected operation is in progress. • **success**: the selected operation succeeded. • **fail**: the selected operation failed.

View the Agent and Diagnostic Software Load Status using the EDM

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

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **File System**.
3. In the work area, click the **Boot Image** tab to view the software status.

Boot Image Tab Field Descriptions

Use the data in the following table to use **Boot Image** tab.

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

Manage POE for a Switch Unit using EDM

Procedure

1. From the Device Physical View, click a switch unit with PoE ports.
2. From the navigation tree, click **Edit**.
3. In the Edit tree, click **Unit**.
4. In the work area, click the **PoE** tab.
5. In the **UsageThreshold%**, type a value.
6. In the **PoweredDeviceDetectType** section, click a radio button.
7. On the toolbar, click **Apply**.

PoE Tab Field Descriptions

Use the data in the following table to use **PoE** tab.

Name	Description
Power(watts)	Displays the total power (in watts) available to the switch.
OperStatus	Displays the power state of the switch: • **on** • **off** • **faulty**
ConsumptionPower(watts)	Displays the power (in watts) being used by the switch.
UsageThreshold%	Specifies a percentage of the total power usage of the switch above which the system sends a trap.

Table continues…

Name	Description
	Important: You must enable the traps (NotificationControlEnable) to receive a power usage trap.
PoweredDeviceDetectType	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: • **802.3at** - IEEE standard for higher PoE (PoE+) • **802.3at and legacy support** -standard in use prior to IEEE 802.at **Important:** The default setting is 802.3at and legacy support. Ensure that this setting matches the setting for the detection type used by the powered devices on this switch.
PowerPresent	Specifies the currently used power source. Available power sources are AC and DC. A value of acOnly indicates that the only power supply is AC. A value of dcOnly indicates that the only power supply is DC. A values of acDc indicates that there are two power supplies; both AC and DC are supplying power.

Configure PoE Power Mode using EDM

Important:

Only the ERS3626GTS-PWR+ operates in two PoE power modes - Fanless mode or Normal mode. The ERS3650GTS-PWR+ operates in Normal mode only.

Use this procedure to configure the PoE power budget mode.

Procedure

1. In the navigation tree, double-click **Power Management** .
2. Click **PoE**.
3. In the work area, click the **Power Mode** tab.
4. Perform one of the following:
   - To enable Low Power Budget Mode and disable fan operation, select **lowPowerBudget**.

   OR
   - To enable High Power Budget Mode and enable fan operation, select **highPowerBudget**.

5. On the toolbar, click **Apply**.

Power Mode Tab Field Descriptions

Use the data in the following table to use the **Power Mode** tab.

Name	Description
PoEPowerMode	Lets you set the power budget mode for switch to be either: • **lowPowerBudget**: Sets the switch PoE budget to 90W max and disables fan operation (Fanless mode). **Note:** lowPowerBudget is supported on the ERS3626GTS-PWR+ platform only. • **highPowerBudget**: Sets the switch PoE budget to 740W max and enables fan operation (Normal mode). DEFAULT: highPowerBudget (Normal mode, fan operates)

Managing Power 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.

Configure PoE for Multiple Switch Units using EDM

Procedure

1. In the navigation tree, click **Power Management**.
2. In the Power Management tree, click **PoE**.
3. In the work area, click the **PoE 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**

PoE Tab Field Descriptions

Use the data in the following table to use **PoE** tab for one or more switches in a stack.

Name	Description
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Enable or disable PoE on this port. By default, PoE is enabled.
DetectionStatus	Displays the operational status of the power-device detecting mode on the specified port: • **disabled**: detecting function disabled. • **searching**: detecting function is enabled and the system is searching for a valid powered device on this port. • **deliveringPower**: detection found a valid powered device and the port is delivering power. • **fault**: power-specific fault detected on port • **test**: detecting device in test mode. • **otherFault** **Important:** It is recommended that test operational status is not used.
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	Specifies the power priority for the specified port to: • critical • high • low
PowerLimit(watts)	Specifies the maximum power that the switch can supply to a port. RANGE: 3 to 32 Watts DEFAULT: 32 Watts
Voltage (volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

View PoE Information for Switch Ports using EDM

Use this procedure to display the PoE configuration for switch ports.

Procedure

1. In the navigation tree, click **Power Management**.
2. In the Power Management tree, click **PoE**.
3. In the work area, click the **Globals – Poe Units** tab.

Globals- PoE Units Tab Field Descriptions

Use the data in the following table to use the **Globals- PoE Units** tab.

Name	Description
Power(watts)	Indicates the total power (in watts) available to the switch.
OperStatus	Indicates the power state of the switch: • **on** • **off** • **faulty** This is a read-only cell.
Consumption Power (watts)	Indicates the power (in watts) being used by the switch. This is a read-only cell.
UsageThreshold%	Indicates the percentage of the total power usage of the preceding switch, to which the system sends a trap. **Important:** You must enable the traps (NotificationControlEnable) to receive a power usage trap.
PowerDeviceDetectionType	Indicates the power detection type that the switch uses to detect a request for power from a device connected to all ports on the switch. Values include: • 802.3at • 802.3atAndLegacySupport

Configuring PoE for Switch Ports using the EDM

Use the information in this section to display and modify PoE configurations for switch ports.

View PoE Information for Switch Ports using EDM

Use this procedure to display the PoE configuration for switch ports.

Procedure

1. In the navigation tree, click **Power Management**.
2. In the Power Management tree, click **PoE**.
3. In the work area, click the **PoE Ports** tab.

PoE Ports Tab Field Descriptions

Use the data in the following table to use the **PoE Ports** tab.

Name	Description
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Enable or disable PoE on this port. By default, PoE is enabled.
DetectionStatus	Displays the operational status of the power-device detecting mode on the specified port: • **disabled**: detecting function disabled. • **searching**: detecting function is enabled and the system is searching for a valid powered device on this port. • **deliveringPower**: detection found a valid powered device and the port is delivering power. • **fault**: power-specific fault detected on port • **test**: detecting device in test mode. • **otherFault** **Important:** Extreme Networks recommends against using the test operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Specifies the power priority for the specified port to: • critical • high • low
PowerLimit(watts)	Specifies the maximum power that the switch can supply to a port.

Table continues…

Name	Description
	RANGE: 3 to 32 Watts DEFAULT: 32 Watts
Voltage (volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

Configure PoE for a Specific Port in EDM

About this task

Use this procedure to modify the PoE configuration for a one or more ports on a specific switch unit.

Procedure

1. From the Device Physical View, select one or more ports on a switch unit.
2. From the navigation tree, double-click **Edit**.
3. From the navigation tree, double-click **Chassis**.
4. From the navigation tree, double-click **Ports**.
5. In the work area, click the **PoE** tab.
6. In the unit port row, select **AdminEnable**.
7. Select a **PowerUpMode** option.
8. Select a **PowerPriority** option.
9. Select a value from the list.
10. Type a value in the **PowerLimit(watts)** field.

PoE Tab Field Descriptions

Use the data in the following table to use **PoE** tab.

Name	Description
AdminEnable	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 802dot3at. Following are the options: • 802.3af—indicates an inrush current of 400 mA to 450 mA. • highInrush—indicates an inrush current as described by the Icut/Ilim (default is 700 mA to 1.0 A).

Table continues…

Name	Description
	• pre802dot3at—indicates an inrush current of 400 mA to 450 mA, which is switched to higher Ilim (700 mA to 1.0 A) within 75 miliseconds, after the port is powered up. • 802dot3at—indicates an inrush current as described by the Icut/Ilim (default is 700 mA to 1.0 A). Where, Ilim represents the highest consumption level possible and Icut 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: • **disabled**: detecting function disabled. • **searching**: detecting function is enabled and the system is searching for a valid powered device on this port. • **deliveringPower**: detection found a valid powered device and the port is delivering power. • **fault**: power-specific fault detected on port • **test**: detecting device in test mode. • **otherFault** **Important:** Extreme Networks recommends against using the test operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices, such as IP phones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Specifies the power priority for the specified port to: • critical • high • low
PowerLimit(watts)	Specifies the maximum power that the switch can supply to a port. RANGE: 3 to 32 Watts DEFAULT: 32 Watts
Voltage(volts)	Indicates the voltage measured in Volts.

Table continues…

Name	Description
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

Configuring PoE for switch or stack ports using EDM

About this task

Use this procedure to modify the PoE configuration for a one or more switch or stack ports.

Procedure

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**.
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** column.
12. Select a value from the list.
13. To configure PoE for other selected ports, repeat steps **4** through **10** .
14. Click **Apply**.

PoE Ports Tab Field Descriptions

Use the data in the following table to use the **PoE Ports** tab.

Name	Description
Unit	Indicates the switch position in a stack.
Port	Indicates the switch port number.
AdminEnable	Enable or disable PoE on this port. By default, PoE is enabled.
DetectionStatus	Displays the operational status of the power-device detecting mode on the specified port: • **disabled**: detecting function disabled.

Table continues…

Name	Description
	• **searching**: detecting function is enabled and the system is searching for a valid powered device on this port. • **deliveringPower**: detection found a valid powered device and the port is delivering power. • **fault**: power-specific fault detected on port • **test**: detecting device in test mode. • **otherFault** **Important:** Extreme Networks recommends against using the test operational status.
PowerClassifications	Classification is a way to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points, and others can be classified according to their power requirements.
PowerPriority	Specifies the power priority for the specified port to: • critical • high • low
PowerLimit(watts)	Specifies the maximum power that the switch can supply to a port. RANGE: 3 to 32 Watts DEFAULT: 32 Watts
Voltage (volts)	Indicates the voltage measured in Volts.
Current(amps)	Indicates the current measured in amps.
Power(watts)	Indicates the power measured in watts.

Configuring IPv6 management using EDM

Use the procedures in this section to configure IPv6.

Configure IPv6 Management globally using EDM

Use this procedure to enable and configure IPv6 Management globally.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.

3. In the work area, click the **Globals** tab.
4. To enable IPv6 Management globally, select the **AdminEnabled** check box.
5. Control the sending of icmpv6 unreachable messages by clicking the **IcmpNetUnreach**.
6. To control the rate of icmpv6 error messages, type a value in the **IcmpErrorInterval** dialog box.
7. On the toolbar, click **Apply**.

Globals Tab Field Descriptions

Use the data in the following table to use **Globals** tab.

Name	Description
AdminEnabled	Enables or disables IPv6 Management globally.
OperEnabled	Indicates if IPv6 Management is operationally enabled or disabled. Values are true (enabled) or false (disabled).
Forwarding	Indicates if IPv6 forwarding is enabled (Forwarding) or disabled (notForwarding). IPv6 forwarding (routing) is not supported, only management interface functions are supported.
DefaultHopLimit	Indicates the default hop limit value.
IcmpNetUnreach	Enables or disables ICMP net unreach.
IcmpRedirectMsg	Indicates if ICMP redirect is enabled (true) or disabled (false).
IcmpErrorInterval	Defines the time (in milliseconds) to wait before sending an ICMP error message. Values range from 0 to 2147483647 ms. A value of 0 means the system does not send an ICMP error message.
IcmpErrorQuota	Indicates the number of ICMP error messages that the system can send during ICMP error interval. A value of 0 means that the system cannot send ICMP error messages.
MulticastAdminStatus	Indicates if the global multicast admin status is enabled (true) or disabled (false).

Configuring IPv6 Interface using EDM

Use the following procedures to create, configure, or view IPv6 interface information.

Create an IPv6 Interface using EDM

Use this procedure to create an IPv6 interface

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6** to open the IPv6 work area.

3. In the work area, click the **Interfaces** tab.
4. Click **Insert**.
5. In the **IfIndex** box, type the interface index of the management VLAN.
6. In the **Identifier** box, type the identifier portion of the address or leave the field blank to use the default MAC-based identifier that is created automatically. This is the IPv6 link-local address.
7. In the **Descr** box, type a description for this IPv6 interface (255 characters maximum length).
8. In the **ReasmMaxSize(MTU)** box, type a value in the MTU field to set the maximum size of an IPv6 packet, in bytes. The range is 1280 to 9600 and the default is 1500.
9. Click the **AdminStatus** box to create and enable the IPv6 interface at the same time.
10. In the **ReachableTime** box, you can type the reachable time. The range is 0 to 3600000 milliseconds.
11. In the **RetransmitTime** box, you can type the retransmit time. The range is 0 to 3600000 milliseconds.
12. Click **Insert**.

Interfaces Tab Field Descriptions

Use the data in the following table to use the **Interfaces** tab.

Name	Description
IfIndex	Specifies the Ifindex of the VLAN.
Identifier	Indicates 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 VLAN 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. The range is from 1280 to 9600, and the default value is 1500.
PhysAddress	Spedifies the media-dependent physical address. 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).

Table continues…

Name	Description
OperStatus	Specifies whether the operation status of the interface is up or down.
ReachableTime	Specifies the time that a neighbor is considered reachable after receiving a reachability confirmation. Values range from 0 to 30000 milliseconds. This is an optional field.
RetransmitTime	Specifies the RetransmitTime, which is the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Values range from 0 to 3600000 milliseconds. This is an optional field.
MulticastAdminStatus	Specifies the multicast status as either True or False.

Configure the IPv6 Management Interface using EDM

Use this procedure to configure the IPv6 management interface, to change IPv6 parameters for the management VLAN and to view IPv6 VLAN configuration information.

Before you begin

- An IPv6 interface must be created and attached to a VLAN before having any kind of connectivity on IPv6. One interface is permitted, and it must be attached to the management vlan. This VLAN can be the default management VLAN 1 or a custom port-based vlan that must be set as management.

Procedure

1. In the navigation tree, double-click **IPv6**.
2. In the IPv6 tree, click **IPv6**.
3. In the work area, click the **Interfaces** tab.
4. To select a VLAN to edit, click the VLAN ID.
5. In the VLAN row, double-click the cell in the **Descr** column.
6. Type a descriptor for the VLAN.
7. In the VLAN row, double-click the cell in the **ReasmMaxSize(MTU)** column.
8. Type an MTU value.
9. In the VLAN row, double-click the cell in the **AdminStatus** column.
10. Select a value from the list—`true` to enable the administration status for the VLAN, or `false` to disable the administration status for the VLAN.
11. In the VLAN row, double-click the cell in the **ReachableTime** column.
12. Type a neighbor reachable time value.
13. In the VLAN row, double-click the cell in the **RetransmitTime** column.

14. Type a retransmit time value.
15. On the toolbar, click **Apply**.

Interfaces Tab Field Descriptions

Use the data in the following table to use the **Interfaces** tab.

Name	Description
IfIndex	Specifies the Ifindex of the VLAN.
Identifier	Indicates the IPv6 address interface identifier, which is a binary string of up to 8 octets in network byte order.
IdentifierLength	Indicates 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	Indicates the Virtual LAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	Indicates the interface port type.
ReasmMaxSize(MTU)	Specifies the MTU for this IPv6 interface. The range is from 1280 to 9600, and the default value is 1500.
PhysAddress	Indicates 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	Indicates whether the operation status of the interface is up or down.
ReachableTime	Specifies the time that a neighbor is considered reachable after receiving a reachability confirmation. Values range from 0 to 30000 milliseconds. This is an optional field.
RetransmitTime	Specifies the RetransmitTime, which is the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Values range from 0 to 3600000 milliseconds. This is an optional field.
MulticastAdminStatus	Indicates the multicast administration status as either true or false.

Graph IPv6 Interface Statistics using EDM

Use this procedure to view and graph IPv6 interface statistics using EDM.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Interfaces** tab.
4. Click **Graph**.
5. To clear the interface statistics counters, click **Clear Counters**.
6. Click the arrow on the **Poll Interval:** box.
7. Select a value from the list.
8. Select **Line Chart**, **Area Chart**, or **Bar Chart** graph type.

Interfaces Graph Tab Field Descriptions

Use the data in the following table to use the **Interfaces Graph** tab.

Name	Description
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	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, and errors discovered in processing their IP options.
InNoRoutes	The number of input IP datagrams discarded because no route could be found to transmit them to their destination.
InAddrErrors	The number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
InUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InTruncatedPkts	The number of input IP datagrams discarded because the datagram frame did not carry enough data.
InDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for

Table continues…

Name	Description
	example, for lack of buffer space). This counter does not include datagrams discarded while awaiting reassembly.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutForwDatagrams	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 includes only those datagrams that were Source-Routed through this entity, and the Source-Route processing was successful.
OutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include datagrams counted in ipForwDatagrams.
OutDiscards	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). This counter includes datagrams counted in ipForwDatagrams if such packets met this (discretionary) discard criterion.
OutFragOKs	The number of IP datagrams that have been successfully fragmented.
OutFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented but could not be. This includes IPv4 packets that have the DF bit set and IPv6 packets that are being forwarded and exceed the outgoing link MTU.
OutFragCreates	The number of output datagram fragments that have been generated because IP fragmentation.
ReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
ReasmOKs	The number of IP datagrams successfully reassembled.
ReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: for example, timed out, and errors). This is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
InMcastPkts	The number of IP multicast datagrams received.

Table continues…

Name	Description
OutMcastPkts	The number of IP multicast datagrams transmitted.

Important:

You can also change the Poll Interval by selecting and clicking on a value from the list. The default value for the Poll Interval is 10 ms.

Configure an IPv6 Address using EDM

Use this procedure to configure an IPv6 address for the switch using EDM.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Addresses** tab.
4. Click **Insert**.
5. Accept the default **IfIndex** value which is the management VLAN of the switch.
6. In the **Addr** box, type an IPv6 address.
7. In the **AddrLen** box, type the IPv6 prefix length.
8. In the **Type** section, click a radio button.
9. Click **Insert**.
10. On the toolbar, click **Apply**.

Addresses Tab Field Descriptions

Use the data in the following table to use the **Addresses** tab.

Name	Description
IfIndex	Specifies the Ifindex of the VLAN.
Addr	Indicates the interface IPv6 address.
AddrLen	Indicates the interface IPv6 prefix length.
Type	Specifies the interface address type. Only unicast is supported for IPv6 management functions.
Origin	Indicates the origin of the interface address. Values include • **other** • **manual**. • **dhcp** • **linklayer**.

Table continues…

Name	Description
	• **random**
Status	Indicates the status of the interface address. Values include • **preferred** • **deprecated**. • **invalid** • **inaccessible**. • **unknown** • **tentative**. • **duplicate**

Configure an IPv6 Loopback Interface using EDM

Use this procedure to configure an IPv6 loopback interface for a switch using EDM.

Note:

You can create only four IPv6 loopback interfaces on a switch/stack.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Loopback** tab.
4. Click **Insert**.

   The **Insert Loopback** dialog box appears.
5. In the **IfIndex** box, type the interface index of the management VLAN.
6. Click the **AdminStatus** box to create and enable the IPv6 interface at the same time.
7. Click **Insert**.

Loopback Tab Field Descriptions

The following table describes the fields on the **Loopback** tab.

Name	Description
IfIndex	Specifies the Ifindex of the VLAN.
Descr	Specifies a text string containing information about the interface. The network management system also sets this string.

Table continues…

Name	Description
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.

IPv6 neighbor cache configuration using EDM

Use the following procedures to configure or view the IPv6 neighbor cache configuration.

Configure the IPv6 Neighbor Cache using EDM

Use this procedure to configure the IPv6 neighbor cache using EDM.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Neighbors** tab.
4. Click **Insert**.
5. Configure IPv6 neighbor cache parameters as required.
6. Click **Insert** to save your changes.

Neighbors Tab Field Descriptions

Use the data in the following table to use the **Neighbors** tab.

Name	Description
IfIndex	A unique value to identify a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN.
NetAddress	The IP address corresponding to the media-dependent physical address.
PhysAddress	The media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
Interface	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.

View the Neighbor Cache using EDM

Use this procedure to view the neighbor cache to discover information about neighbors in your network. Neighbor cache in IPv6 is similar to the IPv4 Address Resolution Protocol (ARP) table. The neighbor cache is a set of entries for individual neighbors to which traffic was sent recently. You make entries on the neighbor on-link unicast IP address, including information such as the link-layer address. A neighbor cache entry contains information used by the Neighbor Unreachability

Detection algorithm, including the reachability state, the number of unanswered probes, and the time the next Neighbor Unreachability Detection event is scheduled.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **Neighbors** tab.

Neighbors Tab Field Descriptions

Use the data in the following table to use **Neighbors** tab.

Name	Description
IfIndex	A unique value to identify a physical interface or a logical interface (VLAN). For the VLAN, the value is the Ifindex of the VLAN.
NetAddress	The IP address corresponding to the media-dependent physical address.
PhysAddress	The media-dependent physical address. The range is 0 through 65535. For Ethernet, this is a MAC address.
Interface	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	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	The type of mapping is as follows: • **Dynamic type**: Indicates that the IP address to the physical address mapping is dynamically resolved using, for example, IPv4 ARP or the IPv6 Neighbor Discovery Protocol.. • **Static type**: Indicates that the mapping is statically configured. • **Local type**: Indicates that the mapping is provided for the interface address.
State	Specifies the Neighbor Unreachability Detection state for the interface when the address mapping in this entry is used. If Neighbor Unreachability Detection is not in use (for example, for IPv4), this object is always unknown. Options include the following: • **reachable**: confirmed reachability

Table continues…

Name	Description
	• **stale**: unconfirmed reachability • **delay**: waiting for reachability confirmation before entering the probe state • **probe**: actively probing • **invalid**: an invalidated mapping • **unknown**: state cannot be determined • **incomplete**:address resolution is being performed

Graph IPv6 Interface ICMP Statistics using EDM

Use this procedure to display and graph IPv6 interface ICMP statistics.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.
3. In the work area, click the **ICMP Stats** tab.
4. To clear the interface statistics counters, click **Clear Counters**.
5. Click the arrow on the **Poll Interval:** box.
6. Select a value from the list.
7. To select data to graph, click a data row under a column heading.
8. 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
InMsgs	Number of ICMP messages received.
InErrors	Number of ICMP error messages received
OutMsgs	Number of ICMP messages sent.
OutErrors	Number of ICMP error messages sent.
Poll Interval	Sets polling interval. Value: 2 to 60 s.

View ICMP Message Statistics using EDM

Use this procedure to view the IPv6 interface ICMP message statistics using EDM

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **IPv6**.

3. In the work area, click the **ICMP Msg Stats** tab.
4. Click **Refresh** to update the ICMP message statistics.

ICMP Msg Stats Tab Field Descriptions

Use the data in the following table to use the **ICMP Msg Stats** tab.

Name	Description
Type	Type of packet received or sent.
InPkts	Number of packets received.
OutPkts	Number of packets sent.

View Global IPv6 TCP Properties using EDM

Use this procedure to view IPv6 TCP properties for the switch.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **TCP/UDP**.
3. In the work area, click the **TCP Globals** tab.
4. Click **Refresh** to update the information.

TCP Globals Tab Field Descriptions

Use the data in the following table to use **TCP Globals** tab.

Name	Description
RtoAlgorithm	Algorithm identifier.
RtoMin	Minimum value in milliseconds.
RtoMax	Maximum value in milliseconds.
MaxConn	Maximum number of connections.

View IPv6 TCP Connections using EDM

Use this procedure to view IPv6 TCP connections using EDM.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **TCP/UDP**.
3. In the work area, click the **TCP connections** tab.
4. Click **Refresh** to update the information.

TCP Connections Tab Field Descriptions

Use the data in the following table to use the **TCP Connections** tab.

Name	Description
LocalAddressType	Local address type
LocalAddress	Local address
LocalAddress Port	Local address port
LocalPort	Local port IP
RemAddress Type	Remote address type
RemAddress	Remote address
RemPort	Remote port IP
State	State • Enabled • Disabled

View IPv6 TCP Listeners using EDM

Use this procedure to view IPv6 TCP listeners using EDM.

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **TCP/UDP**.
3. In the work area, click the **TCP Listeners** tab.
4. Click **Refresh** to update the information.

TCP Listeners Tab Field Descriptions

Use the data in the following table to use the **TCP Listeners** tab.

Name	Description
LocalAddressType	Local address type
LocalAddress	Local address
Local Port	Local port

View IPv6 UDP Endpoints using EDM

Use this procedure to view IPv6 UDP endpoints using EDM

Procedure

1. In the navigation tree, double-click **IPv6** to open the IPv6 navigation tree.
2. In the IPv6 navigation tree, click **TCP/UDP**.
3. In the work area, click the **UDP Endpoints** tab.
4. Click **Refresh** to update the information.

UDP Endpoints Tab Field Descriptions

Use the data in the following table to use the **UDP Endpoints** tab.

Name	Description
LocalAddressType	Local address
LocalAddress	Local address port
Local Port	Local port IP
RemoteAddressType	Remote address type
RemoteAddress	Remote address
RemotePort	Remote port IP
Instance	Indicates the instance.
Process	Indicates the process.

Configure SNTP using EDM

Use this procedure to configure Simple Network Time Protocol (SNTP).

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **SNTP/Clock**.
3. In the work area, click the **Simple Network Time Protocol** tab.
4. In the **PrimaryServerInetAddressType** section, click a radio button.
5. In the **PrimaryServerInetAddress** dialog box, type a value.
6. In the **SecondaryServerInetAddressType** section, click a radio button.
7. In the **SecondaryServerInetAddress** dialog box, type a value.
8. In the **State** section, click a radio button.
9. In the **SyncInterval** dialog box, type a value.
10. In the **ManualSyncRequest** section, click the **requestSync** radio button to synchronize the switch with the NTP server.
11. On the toolbar, click **Apply**.

Simple Network Time Protocol Tab Field Descriptions

Use the data in the following table to use the **Simple Network Time Protocol** tab.

Name	Description
PrimaryServerAddressType	Specifies the primary SNTP server IP address type. Values include ipv4 and ipv6.

Table continues…

Name	Description
PrimaryServerAddress	Specifies the IP address of the primary SNTP server.
SecondaryServerAddressType	Specifies the secondary SNTP server IP address type. Values include ipv4 and ipv6.
SecondaryServerAddress	Specifies the IP address of the secondary SNTP server.
State	Specifies if the switch uses SNTP to synchronize the switch clock to the Coordinated Universal Time (UTC). • **disabled**: the device cannot synchronize its clock using SNTP • **enabled (unicast)**: the device synchronizes to UTC shortly after start time when network access becomes available, and periodically thereafter. **Important:** To clear the PrimaryServerAddress and SecondaryServerAddress, you must first set the State to disabled.
SyncInterval	Specifies the frequency, in hours, that the device attempts to synchronize with the SNTP servers. Values range from 0 to 168. With a value of 0, synchronization occurs only when the switch boots up..
ManualSyncRequest	Specifies that the device will immediately attempt to synchronize with the SNTP servers.
LastSyncTime	Indicates the Coordinated Universal Time (UTC) when the device last synchronized with an SNTP server. This is a read-only value.
LastSyncSourceInetAddressType	Indicates the IP address type of the SNTP server with which this device last synchronized. This is a read-only value.
LastSyncSourceInetAddress	Indicates the IP address of the SNTP server with which this device last synchronized. This is a read-only value.
NextSyncTime	Indicates the UTC at which the next synchronization is scheduled. This is a read-only value.
PrimaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the primary server address. However, synchronization with the secondary server address can still occur. This is a read-only value.
SecondaryServerSyncFailures	Indicates the number of times the switch failed to synchronize with the secondary server address. This is a read-only value.

Table continues…

Name	Description
CurrentTime	Indicates the current switch UTC. This is a read-only value.

Configure Local Time Zone using EDM

Use this procedure to configure the local time zone for the switch geographical location.

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **SNTP/Clock**.
3. In the work area, click the **Time Zone** tab.
4. In the **TimeZone** box, select the time zone offset.
5. In the **TimeZoneAcronym** dialog box, type a time zone acronym.
6. On the toolbar, click **Apply**.

Time Zone Tab Field Descriptions

Use the data in the following table to use the **Time Zone** tab.

Name	Description
TimeZone	Specifies the time zone of the switch, measured as an offset in 15–minute increments from Greenwich Mean Time (GMT).
TimeZoneAcronym	Specifies the time zone acronym.

Configure Daylight Savings time using EDM

Use this procedure to configure the start and end of the daylight savings time period.

Before you begin

Disable the summer time recurring feature.

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **SNTP/Clock**.
3. In the work area, click the **Daylight Saving Time** tab.
4. In the **Offset** dialog box, type a value.
5. In the **TimeZoneAcronym**dialog box, type the time zone acronym.

6. In the **StartYear** dialog box, type a value.
7. In the **StartMonth** box, select a month.
8. In the **StartDay** dialog box, type a value.
9. In the **StartHour** box, select an hour.
10. In the **StartMinutes** dialog box, type a value.
11. Click **Enabled** to enable daylight savings time.
12. Click **Apply**.
13. In the **EndYear** dialog box, type a value.
14. In the **EndMonth** box, select a month.
15. In the **EndDay** dialog box, type a value.
16. In the **EndHour** box, select an hour.
17. In the **EndMinutes** dialog box, type a value.
18. Perform one of the following:
    - Select the **Enabled** check box to enable daylight savings time for the switch.
    - Clear the **Enabled** check box to disable daylight savings time for the switch.
19. Click **Apply**.

Daylight Saving Time Tab Field Descriptions

Use the data in the following table to use on the **Daylight Saving Time** tab.

Name	Description
Offset	Specifies the time in minutes by which you want to change the time when daylight savings begins and ends. The offset is added to the current time when daylight savings time begins and subtracted from the current time when daylight savings time ends.
TimeZoneAcronym	Specifies a time zone acronym.
StartYear	Specifies the year when you want to start the daylight savings time.
StartMonth	Specifies the month of each year when you want to start the daylight savings time.
StartDay	Specifies the day of the particular month when you want to start the daylight savings time.
StartHour	Specifies the hour of the particular day when you want to start the daylight saving time.
StartMinutes	Specifies the minutes of the particular hour when you want to start the daylight savings time.

Table continues…

Name	Description
EndYear	Specifies the year when you want to end the daylight savings time.
EndMonth	Specifies the month of each year when you want to end daylight savings time.
EndDay	Specifies the day of the particular month when you want to end daylight savings time.
EndHour	Specifies the hour of the particular day when you want to end daylight savings time.
EndMinutes	Specifies the minute of the particular hour when you want to end daylight savings time.
Enabled	Enables or disables daylight savings time. **Note:** Before you enable daylight savings time, configure the feature attributes.

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

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **SNTP/Clock**.
3. In the work area, click the **SummerTimeRecurring** tab.
4. Perform one of the following:
   - Select the **Recurring** check box to enable recurring daylight savings time for the switch OR
   - Clear the **Recurring** check box to disable recurring daylight savings time for the switch.
5. In the **RecurringStartMonth** section, click a radio button.
6. In the **RecurringStartWeek** dialog box, type a value.
7. In the **RecurringStartDay** section, click a radio button.
8. In the **RecurringStartHour** dialog box, type a value.
9. In the **RecurringStartMinute** dialog box, type a value.
10. In the **RecurringEndMonth** section, click a radio button.
11. In the **RecurringEndWeek** dialog box, type a value.
12. In the **RecurringEndDay** section, click a radio button.

13. In the **RecurringEndHour** dialog box, type a value
14. In the **RecurringEndMinute** dialog box, type a value.
15. In the **RecurringOffset** dialog box, type a value.
16. On the toolbar, click **Apply**.

SummerTimeRecurring Tab Field Descriptions

Use the data in the following table to use the **SummerTimeRecurring** tab.

Name	Description
Recurring	When selected, enables daylight savings time to recur yearly.
RecurringStartMonth	Specifies the month of each year you want recurring daylight savings time to start.
RecurringStartWeek	Specifies the week of the month you want recurring daylight savings time to start.
RecurringStartHour	Specifies the hour of the particular day you want recurring daylight savings time to start.
RecurringStartMinute	Specifies the minutes of the particular hour you want recurring daylight savings time to start.
RecurringEndMonth	Specifies the month of each year you want recurring daylight savings time to end.
RecurringEndWeek	Specifies the week of the month you want recurring daylight savings time to end.
RecurringEndDay	Specifies the day of the particular month you want recurring daylight savings time to end.
RecurringEndHour	Specifies the hour of the particular day you want recurring daylight savings time to end.
RecurringEndMinute	Specifies the minutes of the particular hour you want recurring daylight savings time to end.
RecurringOffset	Specifies the time in minutes by which you want to change the time when recurring daylight savings begins and ends. The offset is added to the current time when daylight savings time begins and subtracted from the current time when daylight savings time ends.

Initiate a Cable Diagnostic Test using EDM

About this task

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

1. From the **Device Physical View** right-click a port.
2. Click **Edit**.
3. In the work area, click the **TDR** tab.
4. Select **Start Test**.
5. Click **Apply**.

Field Descriptions

Use the data in this table to initiate a cable diagnostic test and help you understand the TDR display.

Name	Description
StartTest	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. • 1—Fail: the cable is experiencing any combination of open and shorted pairs • 2—Normal: the cable is operating normally with no fault found
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: • 1—pairFail • 2—pairNormal • 3—pairOpen • 4—pairShorted • 5—pairNotApplicable • 6—pairNotTested • 7—pairForce • 8—pinShort

Table continues…

Name	Description
	Important: If a 10MB or 100MB link is established without autonegotiation, Pair 1 returns Forced mode. The pair length is meaningless in this case.
Pair1Length	Indicates the length of the first pair in the cable, in meters, measured by the TDR.
Pair2Status	Indicates the status of the second pair in the cable. Values include: • 1—pairFail • 2—pairNormal • 3—pairOpen • 4—pairShorted • 5—pairNotApplicable • 6—pairNotTested • 7—pairForce • 8—pinShort
Pair2Length	Indicates the length of the second pair in the cable, in meters, measured by the TDR.
Pair3Status	Indicates the status of the third pair in the cable. Values include: • 1—pairFail • 2—pairNormal • 3—pairOpen • 4—pairShorted • 5—pairNotApplicable • 6—pairNotTested • 7—pairForce • 8—pinShort
Pair3Length	Indicates the length of the third pair in the cable, in meters, measured by the TDR.
Pair4Status	Indicates the status of the fourth pair in the cable. Values include: • 1—pairFail • 2—pairNormal • 3—pairOpen

Table continues…

Name	Description
	• 4—pairShorted • 5—pairNotApplicable • 6—pairNotTested • 7—pairForce • 8—pinShort
Pair4Length	Indicates the length of the fourth pair in the cable, in meters, measured by the TDR.

Configuring Rear Ports Mode

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

Configure the Rear Ports Mode

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

Procedure

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

Important:

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

Rear Ports Mode Field Descriptions

Use the data in the following table to use the **Rear Ports Mode** tab.

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

Table continues…

Name	Description
	DEFAULT: standalone
RearPortOperMode	Displays the configured operational mode of the rear ports.

Configure a Switch Stack Base Unit

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

Before you begin

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

Procedure

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

Base Unit Info Field Descriptions

Use the data in the following table to use **Base Unit Info** tab.

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

Table continues…

Name	Description
BaseNumPorts	Indicates the number of base ports of the switch
TotalNumPorts	Indicates the total number of ports on the switch
IpAddress	Indicates the base unit IP address
RunningSoftwareVer	Indicates the version of the running software

View Pluggable Ports using EDM

Procedure

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

Stack Info Field Descriptions

Use the data in the following table to use the **Stack Info** tab.

Name	Description
Unit	Displays the stack unit number where the pluggable ports are installed
Port	Displays the port number in the unit where the pluggable port is installed
PortType	Displays the port type
VendorName	Displays the pluggable port vendor name
VendorOUI	Displays the pluggable port vendor's OUI
VendorPartNo	Displays the vendor's part number for the pluggable port
VendorRevision	Displays the vendor's revision number for the pluggable port
VendorSerial	Displays the vendor's pluggable port serial number
HWOptions	Displays hardware options, if present, for the pluggable port
DateCode	Displays the date code for the pluggable port
VendorData	Displays vendor data for the pluggable port
OrderCode	Displays the order code for the pluggable port

Renumber Stack Switch Units

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

Procedure

1. In the navigation tree, click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Stack Numbering** tab.
5. In the unit row, double-click the cell in the **New Unit Number** column.
6. Select a value from the list.
7. On the toolbar, click **Apply**.

   A warning message appears indicating that initiating the renumbering of switch units in a stack results in an automatic reset of the entire stack.

Stack Numbering Tab Field Descriptions

Use the data in the following table to use the **Stack Numbering** tab.

Name	Description
Current Unit Number	Identifies the current switch numbering sequence
New Unit Number	Identifies the updated switch numbering sequence

Display Stored Content

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

Procedure

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

Store Content Tab Field Descriptions

Use the data in the following table to use the **Store Content** tab.

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

Configuring Global Energy Saver using EDM

Use the information in this section to configure Energy Saver (ES) 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

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **EnergySaverEnabled** check box.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

Energy Saver Globals Field Descriptions

Use the data in the following table to use the **Energy Saver Globals** tab.

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

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **EnergySaverEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

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.

Before you begin

- Disable Energy Saver globally.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **PoePowerSavingEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

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.

Before you begin

- Disable Energy Saver globally.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **PoePowerSavingEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

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.

Before you begin

- Disable Energy Saver globally.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Select the **EfficiencyModeEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

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).

Before you begin

- Disable Energy Saver globally.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Globals** tab.
4. Clear the **EfficiencyModeEnabled** check box.
5. Click **Apply**.
6. On the toolbar, you can click **Refresh** to update the work area data display.

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.

Before you begin

- Disable Energy Saver globally.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Schedules** tab.
4. Click **Insert**.
5. To choose a day for the 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 Saverschedule 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**.

Energy Saver Schedules Field Descriptions

Use the data in the following table to use the **Energy Saver Schedules** tab.

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.

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.

Before you begin

- Disable Energy Saver globally.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Saver Schedules** tab.
4. To select a schedule time to edit, click a schedule day.
5. In the schedule day row, double-click the cell in the **ScheduleAction** column.
6. Select a value from the list—**activate** to configure the schedule time as the on time, or **deactivate** to configure the schedule time as the off time.
7. Click **Apply**.

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.

Enable Energy Saver on Individual Ports using EDM

Use the following procedure to turn on Energy Saver for individual ports on a switch or stack.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **ports** tab.
4. Select a **Port**.
5. In the Port row, double-click the cell in the **EnergySaverEnabled** column.
6. Select **true** from the list.
7. Repeat steps 4, 5 and 6 to enable Energy Saver for additional ports as required.
8. Click **Apply**.
9. On the toolbar, you can click **Refresh** to update the work area data display.

Ports Tabs Field Descriptions

Use the data in the following table to use the **Ports** tab.

Name	Description
Port	Specifies the port number.
EnergySaverEnabled	Indicates whether the Energy Saver feature is enabled for the port.

Disable Energy Saver on Individual Ports using EDM

Use the following procedure to turn off Energy Saver for individual ports on a switch or stack.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **ports** tab.
4. Select a **Port**.
5. In the Port row, double-click the cell in the **EnergySaverEnabled** column.
6. Select **false** from the list.
7. Repeat steps 4, 5 and 6 to disable Energy Saver for additional ports as required.
8. Click **Apply**.
9. On the toolbar, you can click **Refresh** to update the work area data display.

View Energy Saver Information using EDM

Use the following procedure to display energy saving information for an individual switch or switches in a stack.

Procedure

1. From the navigation tree, double-click **Power Management**.
2. In the Power Management tree, double-click **Energy Saver**.
3. In the work area, click the **Energy Savings** tab.
4. On the toolbar, you can click **Refresh** update the data.

Energy Savings Field Descriptions

Use the data in the following table to use the **Energy Savings** tab.

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: Link Layer Discovery Protocol (LLDP)

Use the information in this chapter to help you understand Link Layer Discovery Protocol (LLDP) and how to configure LLDP using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

This chapter includes the following sections:

- Link Layer Discovery Protocol fundamentals
- Link Layer Discovery Protocol configuration using CLI
- Link Layer Discovery Protocol configuration using EDM

Link Layer Discovery Protocol fundamentals

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

Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802.3 LAN
- receives network management information from adjacent stations on the same LAN

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

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

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

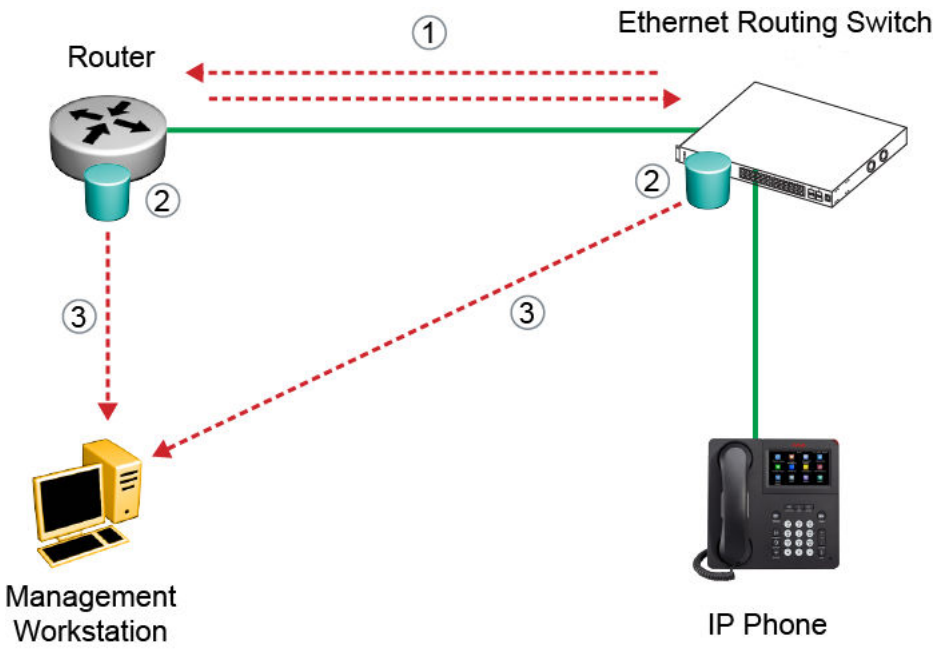


Figure 9: How LLDP works

1. The Ethernet Routing Switch and router advertise chassis or port IDs and system descriptions to each other.
2. The devices store the information about each other in local MIB databases, accessible 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 can also 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 type, length, value (TLV). Each LLDPDU includes the following four mandatory TLVs:

- chassis ID TLV
- port ID TLV
- Time to Live TLV
- End Of LLDPDU TLV

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

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

In addition to the four mandatory TLVs, the switch supports the basic management TLV set. 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 system supported capabilities and enabled capabilities, such as end station, bridge, or router)
- Management Address TLV

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

IEEE 802.3 organizationally-specific TLVs

The optional IEEE 802.3 organizationally-specific TLVs are:

- **MAC/PHY Configuration/Status TLV** indicates the autonegotiation capability and the speed and duplex status of IEEE 802.3 media access control (MAC)/physical (PHY)s
- **Power-Via-MDI (media dependent interface) TLV** indicates the capabilities and current status of IEEE 802.3 physical media dependents (PMDs) that either require or can provide power over twisted-pair copper links

- **Link Aggregation TLV** indicates the current link aggregation status of IEEE 802.3 MACs
- **Maximum Frame Size TLV** indicates the maximum supported 802.3 frame size

Organizationally-specific TLVs for MED devices

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

- Capabilities TLV enables a network element to advertise the LLDP-MED TLVs it is capable of supporting.
- Network Policy Discovery TLV is a fixed length TLV that enables both network connectivity devices and endpoints to advertise VLAN type, VLAN identifier (VID), and Layer 2 and Layer 3 priorities associated with a specific set of applications on a port. In addition, an LLDP-MED endpoint advertises this TLV for supported application types to enable the discovery of specific policy information and the diagnosis of network policy configuration mismatch issues.
- Location Identification TLV allows network connectivity devices to advertise the appropriate location identifier information for an endpoint to use in the context of locationbased 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 LLDPMED endpoint and network connectivity devices. The Extended Power-via-MDI TLV enables the advertisement of fine grained power requirement details, endpoint power priority, and power status for both endpoint and network connectivity devices.
- Inventory TLVs are important in managed Voice over Internet Protocol (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.

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 variables in the LLPDU are modified on the local system (such as system name or management address).

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

TLV system MIBs

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

LLDPDU and TLV error handling

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

Configuring LLDP with CLI

For information about configuring LLDP with CLI, see Configuring Link Layer Discovery Protocol using CLI on page 192.

802.1AB MED network policies

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

You can configure MED network policies on a switch port that has ADAC enabled. The network policies have priority over the ADAC configuration on the port.

When you enable Automatic QoS, the MED network policy changes to DSCP 47 (0x2F) from the user defined DSCP. The DSCP is set to a recognizable value.

An LLDP compliant IP phone uses the received DSCP when receiving voice traffic so that the traffic is recognized by the Automatic QoS and prioritizes accordingly. This feature is automatically enabled when Automatic QoS is enabled.

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 the IP phone supports only 243 levels. If you request a power conservation level higher than 243, the IP phone reverts to its maximum 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 8 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 on switches.

Note:

If your IP Handset uses SIP, 802.1AB (LLDP) TLVs do not provide all information for the IP Phone. You must specify a fileserver IP address TLV so the IP phone can download the SIP

configuration information, because the IP Phone retrieves information related to the SIP domain, port number and transport protocol from the file server.

802.1Q framing TLV

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

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.

802.1AB customization

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

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

- System TLV
- Port Description TLV
- System Name TLV
- System Description TLV
- System Capability TLV
- Management Address TLV
- LLDP MED Capabilities TLV
- Network Policy TLV
- Location Identification TLV
- Extended Power-via-MDI TLV and Inventory TLV

You can also configure the following timers:

- Reinitialization Delay
- Transmit Delay

- Transmit Interval
- Transmit Multiplier Value
- Transmit Hold
- Fast Start Timers
- SNMP Notification Interval

Autotopology

You can enable the Optivity Autotopology protocol on the switch using CLI.

Note:

Autotopology is enabled by default.

FA LLDP extensions

The Fabric Attach (FA) TLVs described in this section are implemented as extensions to the LLDP standard, using the flexible extension mechanism supported by the standard. These TLVs use TLV type 127 as described in the 802.1ab (LLDP) standard.

Extreme Networks Fabric Attach Element TLV

With the Extreme Networks 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 switch 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 Extreme Networks FA Element TLV contains the following data:

- FA Element Type – indicates element capabilities
- FA Element Management VLAN – identifies the management VLAN
- FA Element System ID - unique system identifier used to support element discovery and tracking.
- FA Element State Data - supports the exchange of element state information

The FA Element TLV is included in all LLDPDUs when the FA service is enabled and when the port-level transmission flags associated with this TLV are enabled.

You can view the FA port settings but you cannot update them through the LLDP support. Use the `fa port-enable` command to update the FA port settings.

With the FA service enabled, LLDPDUs containing proprietary Extreme Networks TLVs are transmitted on links that may or may not have Extreme Networks 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 Extreme Networks LLDP TLVs are handled. The other proprietary Extreme Networks TLVs are only included in LLDPUs generated on links that have recognized Extreme Networks elements, specifically Extreme Networks telephony gear, at the far end.

Extreme Networks FA I-SID/VLAN Assignment TLV

With the Extreme Networks FA I-SID/VLAN Assignment TLV, an FA Proxy or FA Client distributes I-SID/VLAN assignments to the FA Server. This information is received, processed and stored by the receiving device so that it is immediately accessible for internal applications.

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 an LLDPDU when complementary FA element devices (FA Proxy, FA Server, or FA Client) are directly connected. The associated port-level transmit flags must be enabled as well.

The Organizationally Specific Extreme Networks FA I-SID/VLAN Assignment TLV contains the following data:

- VLAN ID – identifies the VLAN component of the I-SID-to-VLAN mapping
- I-SID – identifies the I-SID component of the I-SID-to-VLAN mapping
- Status – contains information related to the processing of the I-SID-to-VLAN mapping

Multiple I-SID/VLAN assignments may 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 support 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 may also reject proposed I-SID/VLAN assignments. In this case, the assignment state is updated to rejected.

Extreme Networks TLV Transmit Flags

With the transmit flags, you can choose on a port-level basis, which LLDP TLVs (including the Extreme Networks TLV 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 Extreme Networks TLVs (the PoE Conservation Levels TLV default depends on the devices's PoE support) on all ports. The transmit flags for the FA Element and FA I-SID/VLAN Assignment TLVs default to enabled on the switch, 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 Link Layer Discovery Protocol using CLI

Set LLDP Transmission Parameters

Use this procedure to configure the LLDP transmission parameters or return the parameters to their default values.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

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

   ```
   [default] lldp [tx-interval <5-32768>] [tx-hold-multiplier <2-10>]
   [reinitdelay <1-10>] [tx-delay <1-8192>] [notification-interval
   <5-3600>] [med-fast-start <1-10>]
   ```

Variable definitions

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

Variable	Value
default	Specifies which LLDP parameters you would like to return to their default values when you add one or more of these parameters after the **`default lldp`** command: • tx-interval • tx-hold-multiplier • reinit-delay • tx-delay • notification-interval • med-fast-start If no parameters are specified, the **`default lldp`** command sets all parameters to their default values.
tx-interval *<5–32768*	Sets the interval between successive transmission cycles. DEFAULT: 30
tx-hold-multiplier *<2–10>*	Sets the multiplier for tx-interval used to compute the Time To Live value for the TTL TLV.

Table continues…

Variable	Value
	DEFAULT: 4
reinit-delay *<1–10>*	Sets the delay for re-initialization attempt if the adminStatus is disabled. DEFAULT: 2
tx-delay *<1–8192>*	Sets the minimum delay between successive LLDP frame transmissions. DEFAULT: 2
notification-interval *<5–3600>*	Sets the interval between successive transmissions of LLDP notifications. DEFAULT: 5
med-fast-start *<1–10>*	Sets the vale for MED-Fast-Start. DEFAULT: MED Fast Start repeat count

Enable or Disable LLDP Config Notification

Use this procedure to enable or disable notification when new neighbor information is stored or when existing information is removed.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port> or interface vlan <1-4094>
   ```

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

   ```
   [no] [default] lldp [port <portlist>]config-notification
   ```

   Note:

   The command **`lldp config-notification`** is enabled on the switch by default.

Variable definitions

The following table describes the parameters for the **`lldp config-notification`** command.

Variable	Value
no	Disables config notification.
default	Returns config notification to its default value. DEFAULT: Enabled
port *<portlist>*	Specifies the ports affected by the command.

Configure Optional Management TLVs

Use this procedure to set the optional Management TLVs to be included in the transmitted LLDPDUs

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port> or interface vlan <1-4094>
   ```

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

   ```
   [no] [default] lldp tx-tlv [port <portlist>] [local-mgmt-addr]
   [port-desc] [sys-cap] [sys-desc] [sys-name]
   ```

   Note:

   The command **`lldp tx-tlv local-mgmt-addr port-desc sys-desc sys-name`** is enabled on the switch by default.

Variable definitions

The following table describes the parameters for the **`lldp tx-tlv`** command.

Variable	Value
[no]	Specifies the optional TLVs not to include in the transmitted LLDPDUs. The following parameters can be specified: • local-mgmt-addr • port-desc • sys-cap • sys-desc • sys-name
[default]	Sets the LLDP Management TLVs to their default values
port *<portlist>*	Specifies the ports affected by the command
local-mgmt-addr	Local management address TLV DEFAULT: enable— not included
port-desc	Port description TLV DEFAULT: enable — not included

Table continues…

Variable	Value
sys-cap	System capabilities TLV DEFAULT: enable — not included
sys-desc	System description TLV DEFAULT: enable — not included
sys-name	System name TLV DEFAULT: enable — not included

Configure the IEEE 802.3 Organizationally-Specific TLVs

Use this procedure to specify the optional IEEE 802.3 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port> or interface vlan <1-4094>
   ```

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

   ```
   [no] [default] lldp tx-tlv [port <portlist>] dot 3 [link-
   aggregation] [mac-phy-config-status] [maximum-frame-size] [mdi-
   power-support]
   ```

Variable definitions

The following table describes the parameters for the **`lldp tx-tlv dot3`** command.

Variable	Value
no	Specifies that the optional IEEE 802.3 organizationally-specific TLVs should not be included in the transmitted LLDPDUs.
default	Sets the optional IEEE 802.3 organizationally-specific TLVs to their default values.
port *<portlist>*	Specifies the port affected by the command
link-aggregation	Sets the link aggregation TLV. DEFAULT: false (not included)
mac-phy-config-size	Sets the MAC/PHY configuration or status TLV DEFAULT: false (not included)

Table continues…

Variable	Value
maximum-frame-size	Set the Maximum Frame Size TLV DEFAULT: false (not included)
mdi-power-support	Sets the Power via MDI TLV. Transmission of this TLV is enabled by default only on PoE switch ports. DEFAULT: Enabled

Configure Parameters for LLDP Location Identification

Use the following procedure to set the coordinate-base parameters for LLDP location identification information.

Procedure steps

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

```
lldp location-identification coordinate-base [altitude] [datum]
[latitude] [longitude]
```

Example

```
3549GT (config-if) #lldp location-identification coordinate-base altitude
234 meters datum WGS84
```

Variable definitions

The following table describes the parameters of the **`lldp location-identification coordinate-base`** command.

Variable	Value
altitude *[+ | -] [0-4194303.fracti on] [meters | floors]*	Altitude, in meters or floors.
datum *[NAD83/MLLW | NAD83/NAVD88 | WGS84]*	Reference datum The valid options are: • NAD83/MLLW: North American Datum 1983, Mean Lower Low Water • NAD83/NAVD88: North American Datum 1983, North American Vertical Datum of 1988 • WGS84: World Geodesic System 1984, Prime Meridian Name: Greenwich
latitude *[0-90.00] [NORTH | SOUTH]*	Latitude in degrees, and relative to the equator.
longitude *[0-180.00] [EAST | WEST]*	Longitude in degrees, and relative to the prime meridian.

Configure LLDP Civic Address Parameters

Use the following procedure to set the LLDP civic address parameters.

Procedure steps

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

```
ldp location-identification civic-address country-code [additional-code] [additional-information] [apartment] [block] [building] [city] [city-district ] [county] [floor] [house-number] [house-number-suffix] [landmark] [leading-street-direction] [name] [p.o.box] [place-type] [postal-community-name] [postal/zip-code] [room-number] [state] [street] [street-suffix] [trailing-street-suffix]
```

Example

```
3549GT (config-if)#lldp location-identification civic-address country-code US city Boston street Orlando
```

Variable definitions

The following table describes the parameters of the **`lldp location-identification civic-address`** command.

Variable	Value
`additional-code`	Additional code
`additional-information`	Additional location information
`apartment`	Unit (apartment, suite)
`block`	Neighborhood, block
`building`	Building (structure)
`city`	City, township, shi (JP)
`city-district`	City division, city district, ward
`country-code`	Country code value (2 capital letters)
`county`	County, parish, gun (JP), district (IN)
`floor`	Floor
`house-number`	House number
`house-number-suffix`	House number suffix
`landmark`	Landmark or vanity address
`leading-street-direction`	Leading street direction
`name`	Residence and office occupant
`p.o.box`	Post office box

Table continues…

Variable	Value
place-type	Office
postal-community-name	Postal community name
postal/zip-code	Postal/Zip code
room-number	Room number
state	National subdivisions (state, canton, region)
street	Street
street-suffix	Street suffix
trailing-street-suffix	Trailing street suffix

Configuring the LLDP emergency call service ELIN

Use the following procedure to set the LLDP emergency call service - emergency location identification number (ECS-ELIN).

Procedure steps

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

   ```
   lldp location-identification ecs-elin <ecs-elin>
   ```

   Note:

   <ecs-elin> specifies a 10 to 25 digit numerical string.

Example

```
Switch (config-if)#lldp location-identification ecs-elin 1234567890
```

Configure Optional TLVs for MED Devices

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 Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port> or interface vlan <1-4094>
   ```

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

   ```
   lldp tx-tlv [port <portlist>] med [med-capabilities] [extendedPSE]
   [inventory] [location] [network-policy]
   ```

Note:

The command **`lldp tx-tlv med extendedPSE inventory location med-capabilities network-policy`** is enabled on the switch by default.

Example

```
Switch (config-if)# lldp tx-tlv port  1/12-13 med med-capabilities
Switch (config-if)# lldp tx-tlv port  1/12-13 med extendedPSE
Switch (config-if)# lldp tx-tlv port  1/12-13 med inventory
Switch (config-if)# lldp tx-tlv port  1/12-13 med location
Switch (config-if)# lldp tx-tlv port  1/12-13 med network-policy
```

Variable definitions

The following table describes the parameters for the **`lldp tx-tlv med`** command.

Variable	Value
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). DEFAULT: enabled
extendedPSE	Extended PSE TLV. DEFAULT: enabled
inventory	Inventory TLVs DEFAULT: enabled
location	Location Identification TLV DEFAULT: enabled
network-policy	Network Policy TLV DEFAULT: enabled

Configure LLDPU Transmit and Receive Status

Use this procedure to set the LLDPU transmit and receive status on ports.

Procedure

1. Enter Interface Configuration mode:

   `enable`

   `configure terminal`

   `interface Ethernet` *`<port>`* or `interface vlan` *`<1-4094>`*

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

```
[no] [default] lldp [port <portlist>] status [rxOnly | txAndRx |
txOnly][config-notification]
```

Note:

The command **`lldp status txAndRx config-notification`** is enabled on the switch by default.

Variable definitions

The following table describes the parameters for the **`lldp status`** command.

Variable	Value
[no]	Disables 802.1AB on ports
[default]	Sets the LLDPU transmit and receive status on specified ports to its default value (txAndRx).
port *<portlist>*	Specifies the ports affected by the command.
rxOnly	Enables LLDPU receive only
txAndRx	Enables LLDPU transmit and receive
txOnly	Enables LLDPU transmit only
config-notification	Enables notification when a new neighbor information is stored or when existing information is removed. DEFAULT: enabled

Display Configuration Data for LLDP

Use this procedure to display configuration data for LLDP.

Procedure

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

```
show lldp [local-sys-data] [mgmt-sys-data] [pdu-tlv-size] [stats]
[rx-stats] [tx-stats] [tx-tlv] [neighbor] [neighbor-mgmt-addr]
```

Variable definitions

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

Variable	Value
local-sys-data	Displays 802.1AB local system data
mgmt-sys-data	Displays 802.1AB management data
neighbor	Displays 802.1AB neighbors

Table continues…

Variable	Value
neighbor-mgmt-addr	Displays 802.1AB neighbors management addresses
pdu-tlv-size	Displays 802.1AB tlv in pdu
port<*portlist*>	Specifies the ports affected by the command
rx-stats	Displays 802.1AB RX statistics
stats	Displays LLDP statistics
tx-stats	Displays 802.1AB TX statistics
tx-tlv	Displays 802.1AB TLVs

Display Configuration Data for LLDP Ports

Use this procedure to display configuration data for LLDP ports.

Procedure

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

   ```
   show lldp [port <portlist>] [neighbor] [neighbor-mgmt-addr] [local-sys-data] [rx-stats] [tx-stats] [tx-tlv]
   ```

Example

The example provides a sample output from the **`show lldp port neighbor`** command showing ALL ports.

```
Switch>show lldp port ALL neighbor
-------------------------------------------------------------------------------
                      LLDP neighbor
-------------------------------------------------------------------------------

Port: 2/48  Index: 3                  Time: 0 days, 00:01:30
  ChassisId: MAC address        c4:be:d4:72:16:01
  PortId:    MAC address        c4:be:d4:72:16:30
  SysName:   Lord_1.2
  SysCap:    rB / rB            (Supported/Enabled)
  PortDesc:  Unit 1 Port 47
  SysDescr:
Ethernet Routing Switch 3650GTS-PWR+  HW:B2       FW:6.0.0.3   SW:v6.1.0.043
-------------------------------------------------------------------------------

Port: 1/47  Index: 2                  Time: 0 days, 00:01:31
  ChassisId: MAC address        c4:be:d4:72:16:01
  PortId:    MAC address        c4:be:d4:72:16:71
  SysName:   Lord_1.2
  SysCap:    rB / rB            (Supported/Enabled)
  PortDesc:  Unit 2 Port 48
  SysDescr:
Ethernet Routing Switch 3650GTS       HW:B1       FW:6.0.0.3   SW:v6.1.0.043
-------------------------------------------------------------------------------

Port: 1/1   Index: 1                  Time: 2 days, 00:11:15
```

```
  ChassisId: MAC address        00:1f:da:6c:a4:00
  PortId:    MAC address        00:1f:da:6c:a4:1e
  SysName:   mgmt_Lord        SysCap:    rB / rB            (Supported/Enabled)
  PortDesc:  Port 30
  SysDescr:
Ethernet Routing Switch 2550T         HW:02       FW:1.0.0.15  SW:v4.4.0.011
--------------------------------------------------------------------------

Port: 4/11  Index: 4                  Time: 2 days, 00:24:17
  ChassisId: MAC address        00:1f:da:6c:a4:00
  PortId:    MAC address        00:1f:da:6c:a4:2c
  SysName:   mgmt_Lord
  SysCap:    rB / rB            (Supported/Enabled)
  PortDesc:  Port 44
  SysDescr:
Ethernet Routing Switch 2550T         HW:02       FW:1.0.0.15  SW:v4.4.0.011
--------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 4
```

The example provides a sample output from the **show lldp port neighbor-mgmt-addr** command using Ports 1–3.

```
Switch>show lldp port 1-3 neighbor
--------------------------------------------------------------------------
                     LLDP neighbor-mgmt-addr
--------------------------------------------------------------------------
Port: 2   Index: 2                Time: 0 days, 00:00:58
     ChassisId : MAC address      00:16:ca:da:c4:00
     PortId:     MAC address      00:16:ca:da:c4:30
     MgmtAddr:   IPv4 172.16.120.67
     MgmtOID:    1.3.6.1.4.1.45.3.71.2
     Interface:  type-unknown, number:0
--------------------------------------------------------------------------
Port: 2   Index: 3                Time: 0 days, 00:01:02
     ChassisId : MAC address      00:16:ca:da:c4:00
     PortId:     MAC address      00:16:ca:da:c4:0d
     MgmtAddr:   IPv4 172.16.120.67
     MgmtOID:    1.3.6.1.4.1.45.3.71.2
     Interface:  type-unknown, number:0

--------------------------------------------------------------------------
Port: 2   Index: 4                Time: 0 days, 00:01:03
     ChassisId : MAC address      00:16:0e:9d:28:01
     PortId:     MAC address      00:16:0e:9d:28:19
    MgmtAddr:   IPv4 192.167.130.230
------More   (q=Quit, space/return=Continue)----
```

Important:

To display the neighbor management addresses using the **show lldp port neighbor-mgmt-addr** command, you must configure the connected port of the neighbor to transmit local management address **(lldp tx-tlv [port <portlist>] local-mgmt-addr).**

The example provides a sample output from the **show lldp rx-stats** command.

```
Switch>show lldp rx-stats
--------------------------------------------------------------------------
                           LLDP rx-stats
--------------------------------------------------------------------------
--------------------------------------------------------------------------
Port    Frames        Frames     Frames  TLVs      TLVs           AgeOuts
```

```
Num     Discarded     Errors      Total  Discarded Unrecognized
-------------------------------------------------------------------------
1               0          0          0          0          0          0
2               0          0       2944          0       1105          0
3               0          0          0          0          0          0
4               0          0          0          0          0          0
5               0          0          0          0          0          0
6               0          0          0          0          0          0
7               0          0          0          0          0          0
8               0          0          0          0          0          0
9               0          0          0          0          0          0
10              0          0          0          0          0          0
11              0          0          0          0                     0
12              0          0          0          0          0          0
13              0          0          0          0          0          0
14              0          0          0          0          0          0
15              0          0          0          0          0          0
----More (q=Quit, space/return=Continue)----
```

The example provides a sample output from the **`show lldp tx-stats`** command.

```
Switch>show lldp tx-stats
-------------------------------------------------------------------------
                            LLDP tx-stats
-------------------------------------------------------------------------
-------------------------------------------------------------------------
Port        Frames
-------------------------------------------------------------------------
1                0
2              378
3                0
4                0
5                0
6                0
7                0
8                0
9                0
10               0
11               0
12               0
13               0
14               0
15               0
16               0
----More (q=Quit, space/return=Continue)----
```

The example provides a sample output from the **`show lldp tx-tlv`** command.

```
Switch>show lldp 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
6      true     true     true     true     true
7      true     true     true     true     true
8      true     true     true     true     true
9      true     true     true     true     true
10     true     true     true     true     true
```

```
11      true      true      true      true      true
12      true      true      true      true      true
13      true      true      true      true      true
14      true      true      true      true      true
15      true      true      true      true      true
16      true      true      true      true      true
----More (q=Quit, space/return=Continue)----
```

Variable definitions

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

Variable	Value
port <*portlist*>	Specifies the ports affected by the command
neighbor	Displays LLDP neighbors
neighbor-mgmt-addr	Displays LLDP management addresses for neighbors
local-sys-data	Displays 802.1AB management data
rx-stats	Displays LLDP receive statistics
tx-stats	Displays LLDP transmit statistics
tx-tlv	Displays LLDP transmit TLVs

Configure LLDP MED Network Policies

Use this procedure to configure LLDP network policies on switch ports for MED.

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 {1-4094}]
   ```

Variable definitions

The following table describes the parameters for the **lldp med-network-policies** command.

Variable	Value
port<*portList*>	Specifies a port or list of ports.
voice	Specifies a voice network policy.

Table continues…

Variable	Value
voice-signaling	Specifies a 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 to 63. DEFAULT: 46
priority*{0-7}*	Specifies the 802.1p priority value. Values range from 0 to 7. DEFAULT: 6
tagging*{tagged| untagged}*	Specifies the type of VLAN tagging to apply on the selected switch port or ports. Values include: • tagged: applies a tagged VLAN. • untagged: applies an untagged VLAN or does not support port-based VLANs. **Note:** If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value. DEFAULT: untagged
vlan-id *{1-4094}*	Specifies the VLAN identifier for the selected port or ports. Values range from 1 to 4094. DEFAULT: 0 **Note:** 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.

Restore LLDP MED Network Policies to Default

Use this procedure to restore LLDP MED network policy parameters for switch ports to 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 med-network-policies [port <portList>] voice | voice-signaling
```

Variable definitions

The following table describes the parameters for the **`default lldp med-network-policies`** command.

Variable	Value
port<*portList*>	Specifies a port or list of ports.
voice	Restores voice network policy parameters to default values.
voice-signaling	Restores voice-signaling network policy parameters to default values.

Delete LLDP MED Network Policies

Use this procedure to delete LLDP MED network policy parameters from 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
```

Variable definitions

The following table describes the parameters for the **`no lldp med-network-policies`** command.

Variable	Value
port<*portList*>	Specifies a port or list of ports.
voice	Deletes voice network policy parameters from the selected ports.
voice-signaling	Deletes voice-signaling network policy parameters from the selected ports.

Display LLDP MED Network Policies

Use this procedure to display and verify the LLDP MED network policy configuration for switch ports.

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
   ```

Variable definitions

The following table describes the parameters for the **`show lldp med-network-policies`** command.

Variable	Value
port<*portList*>	Specifies a port or list of ports.
voice	Displays voice network policy configuration information.
voice-signaling	Displays voice-signaling network policy configuration information.

Configure Autotopology

Use this procedure to configure the Optivity Autotopology protocol.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] [default] autotopology
   ```

Variable definitions

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

Variable	Value
no	Disables Autotopology on the switch

Table continues…

Variable	Value
default	Returns Autotopology setting on the switch to the default setting. DEFAULT: Enabled

Display Autotopology Settings

Use this procedure to display information about the Autotopology configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show autotopology settings
   ```

Example

The following figure provides a sample output of the **`show autotopology settings`** command.

```
Switch(config)#sho autotopology settings
Autotopology:  Enabled
Last NMM Table Change:  0 days, 01:55:43
Maximum NMM Table Entries:  298
Current NMM Table Entries:  16
```

Configure the PoE Conservation Level Request TLV

Use this procedure to request a specific power conservation level for an IP phone connected to a switch port.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface Ethernet <port>
   ```
   or
   ```
   interface vlan <1-4094>
   ```

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

   ```
   lldp [port <portlist>] vendor-specific poe-conservation-request-
   level <0-255>
   ```

3. To reset the PoE conservation level TLVs for connected IP phones to the default value, enter the following command:

```
[default] [port <portlist>] lldp vendor-specific poe-conservation-
request-level
```

Important:

Only Ethernet ports on switches that support PoE can request a specific power conservation level for an IP phone.

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific poe—conservation- request-level`** command.

Variable	Value
<0–255>	Specifies the power conservation level to request for a vendor specific PD. With the default value, the switch does not request a power conversation level for an IP phone connected to the port. RANGE: 0 to 255 DEFAULT: 0
port *<portlist>*	Specifies a port or list of ports

Display the Switch PoE Conservation Level Request TLV Configuration

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show lldp [port <portlist>] vendor-specific poe-conservation-
   request-level
   ```

Example

The following figure provides a sample of the **`show lldp vendor-specific poe-conservation-request-level`** command.

```
Switch#show lldp vendor-specific poe-conservation-request-level
-------------------------------------------------------------------------------
              LLDP vendor-specific POE Request Conservation Level
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
      Unit/       POE Request
      Port          Level
-------------------------------------------------------------------------------
      1             0
      2             0
      3             0
      4             0
```

```
      5              0
      6              0
      7              0
      8              0
      9              0
      10             0
      11             0
      12             0
      13             0
      14             0
      15             0
----More (q=Quit, space/return=Continue)----
```

Variable definitions

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

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Display PoE Conservation Level Support TLV Information

Use this procedure to display PoE conservation level 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:

   ```
   show lldp [port <portlist>] neighbor vendor-specific poe-
   conservation
   ```

Configure the Switch Call Server IP Address TLV

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:

Only Ethernet ports on switches that support PoE can request a specific power conservation level for an IP phone.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

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

```
lldp vendor-specific call-server [<1-8>] <A.B.C.D> [[<1-8>]
<A.B.C.D>] [[<1-8>] <A.B.C.D>]
```

3. Delete call server IPv4 addresses configured on the switch by using the following command:

```
default lldp vendor-specific call server <1-8>
```

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific call-server`** command.

Variable	Value
<1–8>	Specifies the call server number. **Note:** When you advertise the IPv4 address of call server 1 only, you do not have to enter a call server number before you enter the IP address.
<A.B.C.D>	Specifies the call server IPv4 address

Display 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.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show lldp vendor-specific call-server
```

Example

The following figure provides a sample of the **`show lldp vendor-specific call-server`** command.

```
Swich#show lldp vendor-specific call-server
------------------------------------------------------------------------
                     LLDP Call Servers IP addresses
------------------------------------------------------------------------
------------------------------------------------------------------------
 Extreme Networks Configured Call Server 1: 192.0.2.1
 Extreme Networks Configured Call Server 2: 192.0.2.2
 Extreme Networks Configured Call Server 3: 192.0.2.3
 ------------------------------------------------------------------------
```

Display IP Phone Call Server IP Address TLV Information

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:

   ```
   show lldp [port <portlist>] neighbor vendor-specific call-server
   ```

Variable definitions

The following table describes the parameters for the **`show lldp neighbor vendor-specific call-server`** command.

Variable	Value
port *<portlist>*	Specifies a port or list of ports

Configure the Switch File Server IP Address TLV

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 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

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

```
lldp vendor-specific file-server [<1-4>] <A.B.C.D> [[<1-4>]
<A.B.C.D>] [[<1-4>] <A.B.C.D>]
```

3. Delete file server IPv4 addresses configured on the switch by using the following command:

```
default lldp vendor-specific file server <1-4>
```

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific file-server`** command.

Variable	Value
<1–4>	Specifies the file server number **Note:** When you advertise the IPv4 address of file server 1 only, you do not have to enter a file server number before you enter the IP address.
<A.B.C.D>	Specifies the file server IPv4 address

Display 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 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:

```
show lldp vendor-specific file-server
```

Display IP Phone File Server IP Address TLV Information

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:

```
show lldp [port <portlist>] neighbor vendor-specific file-server
```

Variable definitions

The following table describes the parameters for the **`show lldp neighbor vendor-specific file-server`** command.

Variable	Value
port *<portlist>*	Specifies a port or list of ports

Configure the 802.1Q Framing TLV

Use this procedure to configure the frame tagging mode for exchanging Layer 2 priority tagging information between the switch and an IP phone.

Before you begin

- Enable LLDP MED capabilities.
- Enable LLDP MED network policies.

Procedure

1. Enter Interface Configuration mode:

```
enable

configure terminal

interface Ethernet <port>
```
or
```
interface vlan <1-4094>
```

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

```
lldp {port <portlist>] vendor-specific dotlq-framing [tagged | non-tagged | auto]
```

3. Set the Layer 2 frame tagging mode to default by using the following command:

```
default lldp [port <portlist>] vendor-specific dotlq-framing
```

Variable definitions

The following table describes the parameters for the **`lldp vendor-specific dotlq-framing`** command.

Variable	Value
port *<portlist>*	Specifies a port or list of ports

Table continues…

Variable	Value
[tagged | non-tagged | auto]	Specifies the frame tagging mode. Values include: • tagged — frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. • non-tagged — frames are not tagged with 802.1Q priority. • auto — an attempt is made to tag frames based on the tagging value the 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. DEFAULT: auto

Display the Switch 802.1Q Framing TLV Configuration

Use this procedure to display the configured Layer 2 frame tagging mode for switch ports.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show lldp [port <portlist>] vendor-specific dotlq-framing
   ```

Variable definitions

The following table describes the parameters for the **`show lldp vendor-specific dotlq-framing`** command.

Variable	Value
port *<portlist>*	Specifies a port or list of ports

Display IP Phone 802.1Q Framing TLV Information

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:

```
show lldp [port <portlist>] neighbor vendor-specific dotlq-framing
```

Variable definitions

The following table describes the parameters for the **`show lldp neighbor vendor-specific dotlq-framing`** command.

Variable	Value
port *<portlist>*	Specifies a port or list of ports

Enable Or Disable Transmit Flag Status

Use this procedure to enable or disable the transmission of optional proprietary Extreme Networks TLVs from switch ports to IP phones.

Important:

The switch transmits configured Extreme Networks TLVs only on ports with the TLV transmit flag enabled.

Procedure

1. Enter Interface Configuration mode:

```
enable

configure terminal

interface Ethernet <port>
```
or
```
interface vlan <1-4094>
```

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

```
[no] [default] lldp tx-tlv [port <portlist>] vendor-specific {[poe—
conservation] [call-server] [file-server] [dotlq-framing]}
```

Variable definitions

The following table describes the parameters for the **`lldp tx-tlv vendor-specific`** command.

Variable	Value
[no]	Disables the transmission of optional proprietary Extreme Networks TLVs from switch ports to IP phones.
[default]	Sets the TLV transmit flag to the default value of true. DEFAULT: enabled

Table continues…

Variable	Value
call-server	Enables the call server TLV transmit flag
dot1q-framing	Enables the Layer 2 priority tagging TLV transmit flag
file-server	Enables the file server TLV transmit flag
poe-conservation	Enables the PoE conservation request TLV transmit flag
port <*portlist*>	Specifies a port or list of ports

Display TLV Transmit Flag Status

Use this procedure to display the status of transmit flags for switch ports on which IP phone support TLVs are configured.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show lldp [port <portlist>] tx-tlv vendor-specific
   ```

Example

The following figure provides a sample of the **`show lldp tx-tlv vendor-specific`** command.

```
Switch#show lldp tx-tlv vendor-specific
--------------------------------------------------------------------------------
                 LLDP port  Vendor-Specific TLVs
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
      Unit/    POE Conservation   Call-Server   File-Server Dot1Q-Framing
      Port        Request
--------------------------------------------------------------------------------
      1           true           true          true          true
      2           true           true          true          true
      3           true           true          true          true
      4           true           true          true          true
      5           true           true          true          true
      6           true           true          true          true
      7           true           true          true          true
      8           true           true          true          true
      9           true           true          true          true
      10          true           true          true          true
      11          true           true          true          true
      12          true           true          true          true
      13          true           true          true          true
      14          true           true          true          true
      15          true           true          true          true
----More (q=Quit, space/return=Continue)----
```

Variable definitions

The following table describes the parameters for the **show lldp tx-tlv vendor-specific** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Display IP Phone IP TLV Configuration

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
   ```

Example

The following figure provides a sample output from the **show lldp port neighbor vendor-specific phone-ip** command.

```
Switch#show lldp port 5 neighbor vendor-specific phone-ip
--------------------------------------------------------------------------------
                       Neighbors LLDP info - TLVs
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Port: 5
      Phone IP:
      Address: 192.1.2.1
      Netmask: 255.255.255.0
      Gateway: 0.0.0.0
```

Variable definitions

The following table describes the parameters for the **show lldp neighbor vendor-specific phone-ip** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports

Configuring Link Layer Discovery Protocol using Enterprise Device Manager

Use the information in this section to configure LLDP properties for local and neighbor systems.

Display the Optional TLVs using EDM

With the LLDP Port tab, you can set the optional TLVs to include in the LLPDUs transmitted by each port.

Procedure

1. In 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 **Port** tab.

Port Tab Field Descriptions

Use the data in the following table to use the **Port** tab.

Name	Description
PortNum	Specifies the Port number.
AdminStatus	Specifies the administratively desired status of the local LLDP agent: • **txOnly**: the LLDP agent transmits LLDP frames on this port and does not store information about the remote systems to which it is connected. • **rxOnly**: the LLDP agent receives but does not transmit LLDP frames on this port. • **txAndRx**: the LLDP agent transmits and receives LLDP frames on this port. • **disabled**: the LLDP agent does not transmit or receive LLDP frames on this port. If the port receives remote system information which is stored in other tables before AdminStatus is disabled, the information ages out..
NotificationEnable	Controls, on a per-port basis, whether notifications from the agent are enabled. • **true**: indicates that notifications are enabled.

Table continues…

Name	Description
	• **false**: indicates that notifications are disabled.
TLVsTxEnable	Sets the optional Management TLVs to be included in the transmitted LLDPDUs: • **portDesc**: Port Description TLV • **sysName**: System Name TLV • **sysDesc**: System Description TLV • **sysCap**: System Capabilities TLV **Important:** The Local Management tab controls Management Address TLV transmission.
CapSupported(med)	Identifies which MED system capabilities are supported on the local system.
TLVsTxEnable(med)	Sets the optional organizationally defined TLVs for MED devices to include in the transmitted LLDPDUs: • **capabilities**: Capabilities TLVs • **networkPolicy**: Network Policy TLVs • **location**: Emergency Communications System Location TLVs • **extendedPSE**: Extended PoE TLVs with PSE capabilitiies • **inventory**: Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, and Asset ID TLVs.
NotifyEnable(med)	A value of **true** enables sending the topology change traps on this port. A value of **false** disables sending the topology change traps on this port.

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).

Display LLDP Global Configuration using EDM

Use the following procedure to display and configure LLDP transmit properties and view remote table statistics.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics work area, click the **802.1AB** tab.
4. In the 802.1AB section, click the **LLDP** tab.
5. On the work area, click the **Globals** tab.
6. In the LLDP section, configure as required.
7. On the toolbar, click **Apply**.

LLDP Globals Tab Field Descriptions

Use the data in the following table to use the **LLDP Globals** tab.

Name	Description
lldpMessageTxInterval	The interval (in seconds) at which LLDP frames are transmitted on behalf of this LLDP agent.
lldpMessageTxHoldMultiplier	The time-to-live value expressed as a multiple of the object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, is expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval *lldpMessageTxHoldMultiplier))

Table continues…

Name	Description
lldpReinitDelay	The delay (in seconds) from when the LLDP Port AdminStatus of a particular port is disabled until reinitialization begins.
lldpTxDelay	The delay (in seconds) between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB.
lldpNotificationInterval	The transmission intervals of LLDP notifications. The agent must not generate more than one notification event in the indicated period. If notification transmission is enabled for particular ports, the suggested default throttling period is 5 seconds.
RemTablesLastChangeTime	The value of the systemUpTime object at the time an entry is created, modified, or deleted in tables associated with the LLDP Remote Systems Data objects, and all LLDP extension objects associated with remote systems.
RemTablesInserts	The number of times the complete set of information is inserted into tables. Any failures occurring during insertion of the information set, which result in deletion of previously inserted information, do not trigger changes. If the failure is the result of a lack of resources, the counter is incremented once.
RemTablesDeletes	The number of times the complete set of information advertised is deleted from tables. 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 from some tables, but not from all tables, are not allowed, and thus, do not change the value of this counter.
RemTablesDrops	The number of times the complete set of information can not be entered into tables because of insufficient resources.
RemTablesAgeouts	The number of times the complete set of information is deleted from tables because the information timeliness interval has expired. This counter increments 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	Set the value (1 to 10) for number of LLDPDUs to be sent at startup to advertise information such as Emergency Call Service Location Identification

Table continues…

Name	Description
	Discovery of endpoints in Voice over Internet Protocol (VoIP) environments.

Display LLDP Transmit Statistics by Port using EDM

Use this procedure to view LLDP transmit statistics by port.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.

   In the Diagnostics tree, click **802.1AB**.
3. In the 802.1AB tree, click **LLDP**.
4. In 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.

Name	Description
PortNum	Specifies the port number
FramesTotal	Specifies the number of LLDP frames transmitted by this LLDP agent on the indicated port

Graph LLDP Transmit Statistics using EDM

Use this procedure to graph LLDP transmit statistics.

Procedure

1. In 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 **TX Stats** tab.
6. From the TX Stats tab, select the port for which you want to display statistics.
7. Click **Graph**. The TX Stats — Graph dialog box appears.
8. Highlight a data column to graph.
9. Click one of the graph buttons.

Display LLDP Receive Statistics by Port using EDM

Use this procedure to view LLDP receive statistics by port.

Procedure

1. In 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 **RX Stats** tab.

RX Stats Tab Field Descriptions

Use the data in the following table to use the **RX Stats** tab.

Name	Description
PortNum	Displays the port number.
FramesDiscardedTotal	Displays 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	Displays the number of invalid LLDP frames received on the port, while the LLDP agent is enabled.
FramesTotal	Displays the number of valid LLDP frames received on the port, while the LLDP agent is enabled.
TLVsDiscardedTotal	Displays the number of LLDP TLVs discarded for any reason.
TLVsUnrecognizedTotal	Displays 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	Displays the counter represents the number of age-outs that occurred on a given port. An age-out is "the number of times the complete set of information advertised by a particular MSAP is deleted from tables in lldpRemoteSystemsData and

Table continues…

Name	Description
	lldpExtensions objects because the information timeliness interval has expired." This counter is similar to lldpStatsRemTablesAgeouts, except that it is on a per-port basis. This enables NMS to poll tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems on the indicated port only. This counter is set to zero during agent initialization. When the admin status for a port changes from disabled to rxOnly, txOnly or txAndRx, the counter associated with the same port is reset to 0. The agent also flushes all remote system information associated with the same port. This counter is incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, does not change the value of this counter.

Graph LLDP Receive Statistics using EDM

Use this procedure to graph LLDP receive statistics.

Procedure

1. In 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 **RX Stats** tab.
6. From the RX Stats tab, select the port for which you want to display statistics.
7. Click **Graph**. The RX Stats — Graph dialog box appears.
8. Highlight a data column to graph.
9. Click one of the graph buttons.

Display the LLDP Properties for the Local System using the EDM

Use this procedure to view LLDP properties for the local system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.

2. In the Edit tree, double-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 System** tab.

Local System Tab Field Descriptions

Use the data in the following table to use the **Local System** tab.

Name	Description
AssetID	Displays the vendor-specific asset tracking identifier.
ChassisIdSubtype	Displays the type of encoding used to identify the local system chassis. Can be: • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Displays the Chassis Identification.
DeviceClass	Displays the MED device class
DeviceType	Displays the type of Power-via-MDI (Poe). Can be: • pseDevice • pdDevice • none
FirmwareRev	Displays vendor-specific firmware revision string.
HardwareRev	Displays vendor-specific hardware revision string.
MfgName	Displays vendor-specific manufacturer name.
ModelName	Displays vendor-specific model name.
PDPowerPriority	Defines the priority as: • critical • high • low
PDPowerReg	Specifies the value of the power required (in units of 0.1 watts) by a PoweredDevice (PD).
PDPowerSource	Defines the type of Power Source.

Table continues…

Name	Description
PSEPowerSource	Defines the type of PSE Power Source as Primary or Back-up.
SerialNum	Displays vendor-specific serial number.
SoftwareRev	Displays vendor-specific software revision string.
SysName	Displays local system name.
SysDesc	Displays local system description.
SysCapSupported	Identifies the system capabilities supported on the local system.
SysCabEnabled	Identifies the system capabilities enabled on the local system.

Display the LLDP Port Properties for the Local System using EDM

Use this procedure to view LLDP port properties for the local system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 Port** tab.

Local Port Tab Field Descriptions

Use the data in the following table to use the **Local Port** tab.

Name	Description
PortNum	Displays the Port number.
PortIdSubtype	Displays the type of port identifier encoding used in the associated PortId object. Can be: • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local

Table continues…

Name	Description
PortId	Displays the string value used to identify the port component associated with a given port in the local system.
PortDesc	Displays 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.

Managing LLDP using EDM

Use the following procedures to display, enable, or disable local management information.

Display LLDP Local Management Information using EDM

Use this procedure to display LLDP management properties for the local system.

Procedure

1. In 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 **LLDP**.
5. In the work area, click the **Local Management** tab.

Local Management tab field descriptions

The following table describes the fields on 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. **Note:** If you configure both IPv4 and IPv6 management addresses, the switch displays each on a separate row.
AddrLen	Identifies the numbering method used to define the interface number associated with the remote system.

Table continues…

Name	Description
AddrIfSubtype	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.
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	Identifies the ports on which the local system management address TLVs are transmitted in the LLPDUs.

Enable or Disable LLDP Management Address TLV Transmission using EDM

Use this procedure to enable or disable the transmission of Management Address TLVs on the local system.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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**.

Display LLDP Properties for the Remote System using the EDM

Use this procedure to view LLDP properties for the remote system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Neighbor** tab.

Neighbor Tab Field Descriptions

Use the data in the following table to use the **Neighbor** tab.

Name	Description
TimeMark	Displays the TimeFilter for this entry. See the TimeFilter textual convention in IETF RFC 2021 for details about TimeFilter.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign montonically increasing index values to new entries, starting with one, after each restart.
ChassisIdSubtype	Displays the type of encoding used to identify the remote system chassis: • chassisComponent • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • local
ChassisId	Specifies 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	Displays the remote system name.
SysDesc	Displays the remote system description.

Table continues…

Name	Description
PortIdSubtype	Displays the type of encoding used to identify the remote port. • interfaceAlias • portComponent • macAddress • networkAddress • interfaceName • agentCircuitId • local
PortId	Displays remote port ID.
PortDesc	Displays remote port description.

Display LLDP Management Properties for the Remote System using EDM

Use this procedure to display LLDP management properties for the remote system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Neighbor Mgmt Address** tab.

Neighbor Mgmt Address Tab Field Descriptions

Use the data in the following table to use the **Neighbor Mgmt Address** 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.

Table continues…

Name	Description
AddrSubtype	Indicates the type of encoding used in the associated Addr object.
Addr	Indicates the management address associated with the remote system. The switch supports IPv4 and IPv6 management addresses. **Note:** If you configure both IPv4 and IPv6 management addresses, the switch displays each on a separate row.
AddrIfSubtype	Indicates the numbering method used to define the interface number associated with the remote system. • unknown • ifindex • systemPortNumber
AddrIfId	Indicates the integer value used to identify the interface number of the management address component associated with the remote system.
AddrOID	Indicates the value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.

Display Specific Properties for the Remote System organizationally using EDM

Use this procedure to view organizationally specific properties for the remote system using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Organizational Defined Info** tab.

Organizational Defined Info Tab Field Descriptions

Use the data in the following table to use the **Organizational Defined Info** tab.

Name	Description
TimeMark	Displays the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each restart.
OrgDefInfoOUI	Displays the Organizationally Unique Identifier (OUI), as defined in IEEE 802-2001, which is a 24 bit (three octets) globally unique assigned number referenced by various standards, of the information received from the remote system.
OrgDefInfoSubtype	Displays 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 restart. It is unlikely that the lldpRemOrgDefInfoIndex wraps between restarts.
OrdDefInfo	Identifies the organizationally defined information of the remote system. The encoding for this object is the same as that defined for SnmpAdminString TC.

Managing LLDP local MED Policies

You can use the information in this section to create, configure, and delete local LLDP MED policies for switch ports.

Configure LLDP Local MED Policies for Ports

Use this procedure to display and modify local LLDP MED policy configurations for switch ports..

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Local Policy** tab.
6. Configure Local Policy parameters for switch ports as required.
7. On the toolbar, click **Apply**.
8. On the toolbar, you can click **Refresh** to verify the Local Policy configuration.

Port MED Local Policy Tab Field Descriptions

Use the data in the following table to use the **Port MED Local Policy** tab.

Name	Description
PortNum	Indicates the port number.This is a read-only cell.
PolicyAppType	Indicates the policy application type. This is a read-only cell.
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. DEFAULT: 0
PolicyPriority	Indicates the value of the 802.1p priority which is associated with the local port. DEFAULT: 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 given port on the local system. DEFAULT: 46
PolicyTagged	Indicates whether the application is using a tagged VLAN, untagged VLAN, or does not support a port based VLAN operation.

Create a Port LLDP Local MED Policy

Use this procedure to create a new LLDP local MED policy for a switch port.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the Port MED work area, click the **Local Policy** tab.
6. Click **Insert**.
7. Configure the local MED policy as required.
8. Click **Insert**.

Field Descriptions

Name	Description
PortNum	Specifies the port on which to configure LLDP MED policies.
PolicyAppType	Specifies the policy application type. • voice — selects the voice network policy • voiceSignaling — selects the voice signalling network policy. • guestVoice • guestVoiceSignaling • softPhoneVoice • videoconferencing • streamingVideo • videoSignaling
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.

Table continues…

Name	Description
PolicyTagged	Specifies the type of VLAN tagging to apply on the selected switch port or ports. • when selected — uses a tagged VLAN • when cleared — uses an untagged VLAN or does not support port-based VLANs. If you select untagged, the system ignores the VLAN ID and priority values, and recognizes only the DSCP value.

Delete a Port LLDP Local MED Policy

Use this procedure to delete an LLDP local MED policy from a switch port.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostic tree, double-click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the Port MED work area, click the **Local Policy** tab.
6. To select a policy to delete, click the **PortNum**.
7. On the toolbar, click **Delete**.

Managing Local Location Information using EDM

Use the information in this section to view and add local location information for remote network devices connected to a switch.

Display Device Location Information using EDM

Use this procedure to display local location information for remote network devices connected to a switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Local Location** tab.

Local Location Tab Field Descriptions

Use the data in the following table to use the **Local Location** tab.

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, as one of the following: • **unknown** • **coordinateBased**: location information is based on geographical coordinates of the remote device • **civicAddress**: location information is based on the civic address of the remote device • **elin**: location information is based on the Emergency Location Information Number (ELIN) of the remote device
LocationInfo	Displays local location information advertised by the remote device. The information displayed in this cell is directly associated with the location subtype value.

Add ELIN based Device Location Information using EDM

Use this procedure to add information to the local location table for remote network devices connected to a switch, based on an Emergency Location Information Number (ELIN).

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In 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 10–25 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, based on geographical coordinates and a civic address.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In 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**.

Local Location Tab Field Descriptions

Use the data in the following table to use the **Local Location** tab.

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).
Map Datum	Specifies the map reference datum. Values are as follows: • **WGS84**: World Geodesic System 1984, Prime Meridian Name: Greenwich • **NAD83/NAVD88**: North American Datum 1983/ North American Vertical Datum of 1988 • **NAD83/MLLW**: North American Datum 1983 / Mean Lower Low Water

Display local PSE PoE information using EDM

Use this procedure to view the local Power over Ethernet (PoE) Power Supply for Ethernet (PSE) information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Local PoE PSE** tab.
6. Click **Refresh** to update the information.

Local PoE PSE Tab Field Descriptions

Use the data in the following table to use the **Local PoE PSE** tab.

Name	Description
PortNum	Displays the port number.
PSEPortPowerAvailable	Displays the power available over the PoE port in watts.
PSEPortPDPriority	Displays the priority rating for the port.

Display Neighbor Capabilities using EDM

Use this procedure to view Neighbor Capabilities information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Capabilities** tab.
6. Click **Refresh** to update the information.

Neighbor Capabilities Tab Field Descriptions

Use the data in the following table to use the **Neighbor Capabilities** tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
Local PortNum	Identifies the local port on which the remote system information is received.

Table continues…

Name	Description
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
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	Provides the remote MED device class.

Display Neighbor Policy using EDM

Use this procedure to view Neighbor Policy information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Policy** tab.
6. Click **Refresh** to update the information.

Neighbor Policy Tab Field Descriptions

Use the data in the following table to use the **Neighbor Policy** tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PolicyAppType	Shows the policy application type.
PolicyVlanID	Displays an extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 is used to define a valid PVID. A value

Table continues…

Name	Description
	of 0 is used if the device is using priority tagged frames, meaning that only the 802.1P priority level is significant and that the default VID of the ingress port is being used instead. A value of 4095 is reserved for implementation use.
PolicyPriority	Indicates the value of the 802.1P priority which is associated with the remote system connected to the port.
PolicyDscp	Displays the value of the Differentiated Service Code Point (DSCP) as defined in IETF RFC 2474 and RFC 2475 that is associated with the remote system connected to the port.
PolicyUnknown	A value of **true** indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID, the Layer 2 priority, and the DSCP value fields are ignored. A value of **false** indicates that this network policy is defined.
PolicyTagged	A value of **true** indicates that the application is using a tagged VLAN. A value of **false** indicates that for the specific application, the device is using an untagged VLAN or does not support a port based VLAN operation. In this case, both the VLAN ID and the Layer 2 priority fields are ignored, and only the DSCP value has relevance.

Managing Neighbor Location Information using EDM

Use the information in this section to view and add neighbor location information for network devices connected to a switch.

Display Neighbor Location Information using EDM

Use this procedure to view Neighbor Location information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Location** tab.
6. Click **Refresh** to update the information.

Neighbor Location Tab Field Descriptions

Use the data in the following table to use the **Neighbor Location** tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
LocationSubtype	Displays the location subtype advertised by the remote device, as one of: • **unknown** • **coordinateBased**: location information is based on geographical coordinates of the remote device • **civicAddress**: location information is based on the civic address of the remote device • **elin**: location information is based on the Emergency Location Information Number (ELIN) of the remote device
LocationInfo	Displays local location information advertised by the remote device. The information displayed in this cell is directly associated with the location subtype value.

Add Coordinate-based Neighbor Location Information using EDM

Use this procedure to add coordinate-based location information to the neighbor location table.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Location** tab.
6. In the table, select a location with the **LocationSubtype** listed as **coordinateBased**.
7. In the toolbar, click the **Location Details** button.
8. Insert coordinate-based neighbor location information criteria.
9. Click **Close**.

Add Civic Address Location Information using EDM

Use this procedure to add civic address-based location information to the neighbor location table.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Location** tab.
6. In the table, select a location with the **LocationSubtype** listed as **civicAddress**.
7. In the toolbar, click **Location Details** .
8. Insert civic address-based neighbor location information criteria.
9. Click **Close**.

Display Neighbor PoE Information using EDM

Use this procedure to view Neighbor Power over Ethernet (PoE) information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor PoE** tab.
6. Click **Refresh** to update the information.

Neighbor PoE Tab Field Descriptions

Use the data in the following table to use the **Neighbor PoE** tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an 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.
PoEDeviceType	Defines the type of Power-via-MDI (Power over Ethernet) advertised by the remote device as follows: • **pseDevice**: Indicates that the device is advertised as a Power Sourcing Entity (PSE). • **pdDevice**: Indicates that the device is advertised as a Powered Device (PD). • **none**: Indicates that the device does not support PoE.

Display Neighbor PoE PSE Information using EDM

Use this procedure to view Neighbor Power over Ethernet (PoE) Power Supply for Ethernet (PSE) information using EDM.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor PoE PSE** tab.
6. Click **Refresh** to update the information.

Neighbor PoE PSE Tab Field Descriptions

Use the data in the following table to use the **Neighbor PoE PSE** tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
PSEPowerAvailable	Specifies the power available (in units of 0.1 watts) from the PSE connected remotely to this port.

Table continues…

Name	Description
PSEPowerSource	Defines the type of PSE Power Source advertised by the remote device, as follows: • **primary**: Indicates that the device advertises its power source as primary. • **backup**: Indicates that the device advertises its power source as backup.
PSEPowerPriority	Specifies the priority advertised by the PSE connected remotely to the port, as follows: • **critical**: Indicates that the device advertises its power priority as critical, see RFC 3621. • **high**: Indicates that the device advertises its power priority as high, see RFC 3621. • **low**: Indicates that the device advertises its power priority as low, see RFC 3621.

Display Neighbor PoE PD Information using EDM

Use this procedure to view Neighbor Power over Ethernet (PoE) Powered Device (PD) information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor PoE PD** tab.
6. Click **Refresh** to update the information.

Neighbor PoE PD Tab Field Descriptions

Use the data in the following table to use the **Neighbor PoE PD** tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an 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.
PDPowerReq	Specifies the value of the power required (in units of 0.1 watts) by a Powered Device (PD) connected remotely to this port.
PDPowerSource	Defines the type of Power Source advertised as being used by the remote device, as follows: • **fromPSE**: Indicates that the device advertises its power source as received from a PSE. • **local**: Indicates that the device advertises its power source as local. • **localAndPSE**: Indicates that the device advertises its power source as using both local and PSE power.
PDPowerPriority	Specifies the priority advertised by the PD connected remotely to the port, as follows: • **critical**: Indicates that the device advertises its power priority as critical, see RFC 3621. • **high**: Indicates that the device advertises its power priority as high, see RFC 3621. • **low**: Indicates that the device advertises its power priority as low, see RFC 3621.

Display Neighbor Inventory Information using EDM

Use this procedure to view Neighbor Inventory information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **802.1AB**.
4. In the 802.1AB tree, click **Port MED**.
5. In the work area, click the **Neighbor Inventory** tab.
6. Click **Refresh** to update the information.

Neighbor Inventory Tab Field Descriptions

Use the data in the following table to use the **Neighbor Inventory** tab.

Name	Description
TimeMark	Specifies the TimeFilter for this entry.
LocalPortNum	Identifies the local port on which the remote system information is received.
Index	Displays an arbitrary local integer value used by this agent to identify a particular MSAP. An agent is encouraged to assign monotonically increasing index values to new entries, starting with one, after each reboot.
HardwareRev	Displays the vendor-specific hardware revision string as advertised by the remote device.
FirmwareRev	Displays the vendor-specific firmware revision string as advertised by the remote device.
SoftwareRev	Displays the vendor-specific software revision string as advertised by the remote device.
SerialNum	Displays the vendor-specific serial number as advertised by the remote device.
MfgName	Displays the vendor-specific manufacturer name as advertised by the remote device.
ModelName	Displays the vendor-specific model name as advertised by the remote device.
AssetID	Displays the vendor-specific asset tracking identifier as advertised by the remote device.

Transmitting TLVs using EDM

Use the information in this section to view or enable the transmission of optional proprietary Extreme Networks TLVs from switch ports to IP phones.

Display the TLV Transmit Flag Status using EDM

Use this procedure to view the status of transmit flags for switch ports on which IP phone support TLVs are configured.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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.

Port Config Tab Field Descriptions

Use the data in the following table to use the **Port Config** tab.

Name	Description
poeConservationLevel	Enables or disables the TLV for requesting a specific power conservation level for an IP phone connected to the switch port. **Important:** 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.

Enable or Disable TLV Transmit Flags using EDM

Use this procedure to enable or disable the transmission of optional proprietary Extreme Networks TLVs from switch ports to IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **PortNum**.
7. In the port row, double-click the cell in the **TLVsTxEnable** column.
8. Select a check box to enable a TLV.

   OR

   Clear a check box to disable a TLV.
9. Click **Ok**.
10. On the toolbar, click **Apply**.

Port Config Tab Field Descriptions

Use the data in the following table to use the **Port Config** tab.

Name	Description
poeConservationLevel	Enables or disables the TLV for requesting a specific power conservation level for an IP phone connected to the switch port. **Important:** 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.

Configuring and Displaying PoE Conservation Level and 802 Framing TLV management using EDM

Use the following procedures to display or configure PoE conservation levels and 802.1Q framing TLV.

Configure the PoE Conservation Level Request TLV using EDM

Use this procedure to request a specific power conservation level for an IP phone connected to a switch port.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **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**.

Local Port Tab Field Descriptions

Use the data in the following table to use the **Local Port** tab.

Name	Description
PoeConsLevelRequest	Specifies the power conservation level to request for a vendor-specific PD. With the default value, the switch does not request a power conservation level for an IP phone connected to the port. RANGE: 0 to 255 DEFAULT: 0

Display 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

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Local Port** tab.

Local Port Tab Field Descriptions

Use the data in the following table to use the **Local Port** tab.

Name	Description
Dot1QFramingRequest	Specifies the frame tagging mode. Values include: • **tagged**: frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. • **non-tagged**: frames are not tagged with 802.1Q priority. • **auto**: an attempt is made to tag frames based on the tagging value the 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.

Table continues…

Name	Description
	DEFAULT: auto
PoeConsLevelRequest	Specifies the power conservation level to request for a vendor-specific PD. With the default value, the switch does not request a power conservation level for an IP phone connected to the port. RANGE: 0 to 255 DEFAULT: 0

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

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **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**.

Local Port Tab Field Descriptions

Use the data in the following table to use the **Local Port** tab.

Name	Description
Dot1QFramingRequest	Specifies the frame tagging mode. Values include: • **tagged**: frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. • **non-tagged**: frames are not tagged with 802.1Q priority. • **auto**: an attempt is made to tag frames based on the tagging value the 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.

Name	Description
	DEFAULT: auto

Managing Local Call Server using the EDM

Use the following procedures to display or configure local call server features.

Display 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

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Local Call Servers** tab.

Local Call Servers Tab Field Descriptions

Use the data in the following table to use the **Local Call Servers** tab.

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 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

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **LocalCallServers** 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**.

Local Call Servers Tab Field Descriptions

Use the data in the following table to use the **Local Call Servers** tab.

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

Managing Local File Server using EDM

Use the following procedures to manage local file server information.

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 file 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.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **LocalFileServers** tab.
6. To select a port, click the **FileServerNum**.

7. In the port row, double-click the cell in the **FileServerAddress** column.
8. Type an IP address in the box.
9. On the toolbar, click **Apply**.

Local File Servers Tab Field Descriptions

Use the data in the following table to use the **Local File Servers** tab.

Name	Description
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Defines file server IP address to advertise.

Display 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

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Local File Servers** tab.

Local File Servers Tab Field Descriptions

Use the data in the following table to use the **Local File Servers** tab.

Name	Description
FileServerNum	Displays the file server number.
FileServerAddressType	Displays the file server IP address type.
FileServerAddress	Displays the defined file server IP address.

Display 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

1. In the navigation tree, double-click **Edit**.

2. In the Edit tree, double-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 **Neighbor Devices** tab.

Neighbor Devices Tab Field Descriptions

Use the data in the following table to use the **Neighbor Devices** tab.

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.
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.

Display Remote Call Server IP Address TLV Information using EDM

Use this procedure to display remote call server IP address information received on switch ports from an IP phone.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Neighbor Call Servers** tab.

Neighbor Call Servers Tab Field Descriptions

Use the data in the following table to use the **Neighbor Call Servers** tab.

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.

Display Remote File Server IP Address TLV Information using EDM

Use this procedure to display remote file server IP address information received on switch ports from an IP phone.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Neighbor File Servers** tab.

Neighbor File Servers Tab Field Descriptions

Use the data in the following table to use the **Neighbor File Servers** tab.

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 fileserver IP address used by the IP phone connected to the switch port.

Display 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

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Neighbor PoE** tab.

Neighbor PoE Tab Field Descriptions

Use the data in the following table to use the **Neighbor PoE** tab.

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.

Display 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

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Neighbor Dot1Q** tab.

Neighbor Dot1Q Tab Field Descriptions

Use the data in the following table to use the **Neighbor Dot1Q** tab.

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 swtich port. Values include: • **tagged**: frames are tagged based on the tagging value the IP phone receives with the LLDP-MED Network Policy TLV. • **non-tagged**: frames are not tagged with 802.1Q priority. • **auto**: an attempt is made to tag frames based on the tagging value the 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. DEFAULT: auto

Display Remote IP TLV Information using EDM

Use this procedure to display IP address configuration information received on switch ports from connected IP phones.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-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 **Neighbor IP Phone** tab.

Neighbor IP Phone Tab Field Descriptions

Use the data in the following table to use the **Neighbor IP Phone** tab.

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 the gateway IP address for the IP phone connected to the switch port.

Chapter 5: 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+ 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.

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, an event is added to the server log. The switch then 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 user name length is 15 characters.

  Note:
  The created user name overrides the read-write (rw) user name.

  The supported range for password length is 10 to 15 characters. The password must include a minimum of two uppercase characters, two lowercase characters, two numbers and two special characters (from the list: `!@#$%^*()&`).

- 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 256 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

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 following configuration using ZTP+:

- Link Aggregation Control Protocol (LACP)
- Multiple Spanning Tree Protocol (MSTP)
- Multiple VLAN Registration Protocol (MVRP)
- Power over Ethernet (PoE)
- Management VLAN

Note:
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.

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 cli password
     ```

   - 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     None             0x0000  Yes    IVL     Yes
        Port Members: ALL
100  VLAN #100            Port     None             0x0000  Yes    IVL     No
        Port Members: NONE
200  VLAN #200            Port     None             0x0000  Yes    IVL     No
        Port Members: NONE
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:
Views for Authenticated and Encrypted Access:
Read View:
Write View:
Notify View:
```

View interface status and configuration:

```
Switch:1#show interfaces

              Status
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
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 cli password
Access Login     Username / Password
------ --------- ----------------------------------
RW     RW        ztp-admin / ***************
RO     RO        RO / ***************
```

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
```

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.

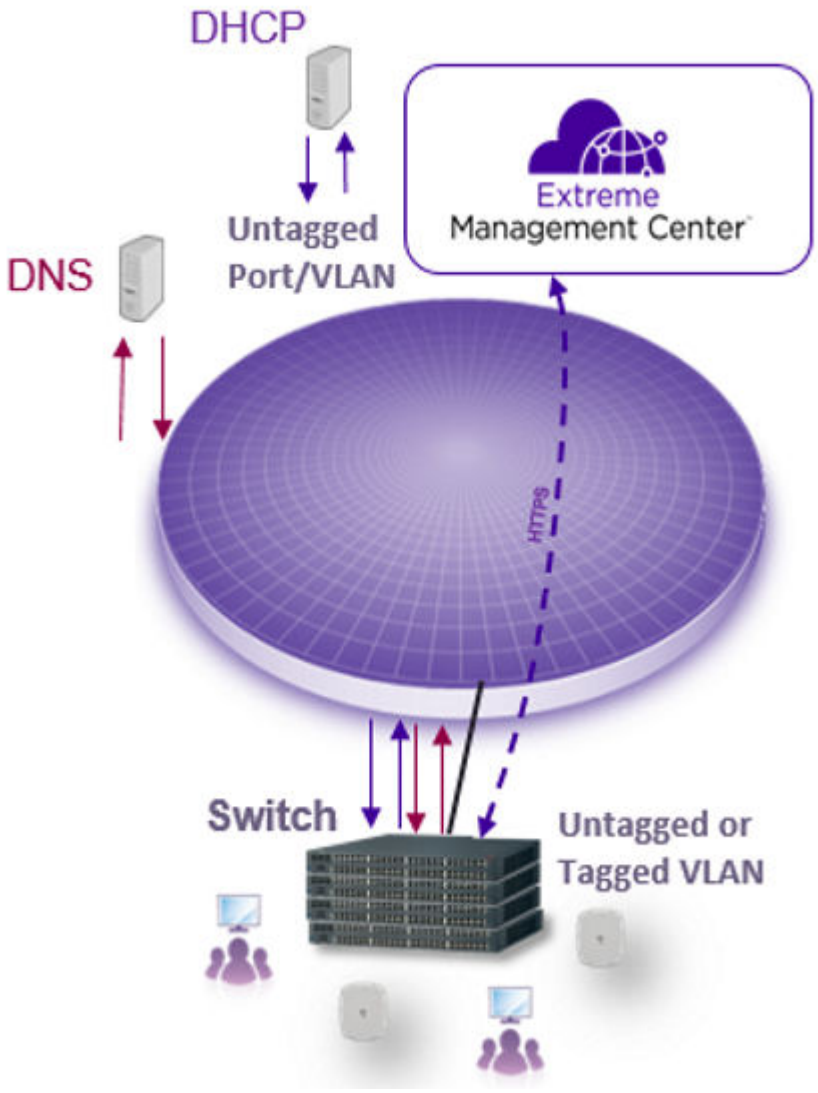


Figure 10: A simple ZTP+ solution

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 cli password`
- 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 is 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:R0D.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:R0D.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.
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

              Status
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 cli password
Access Login     Username / Password
------ --------- ----------------------------------
RW     RW        ztp-admin / ***************
RO     RO        RO / ***************
```

- 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-`

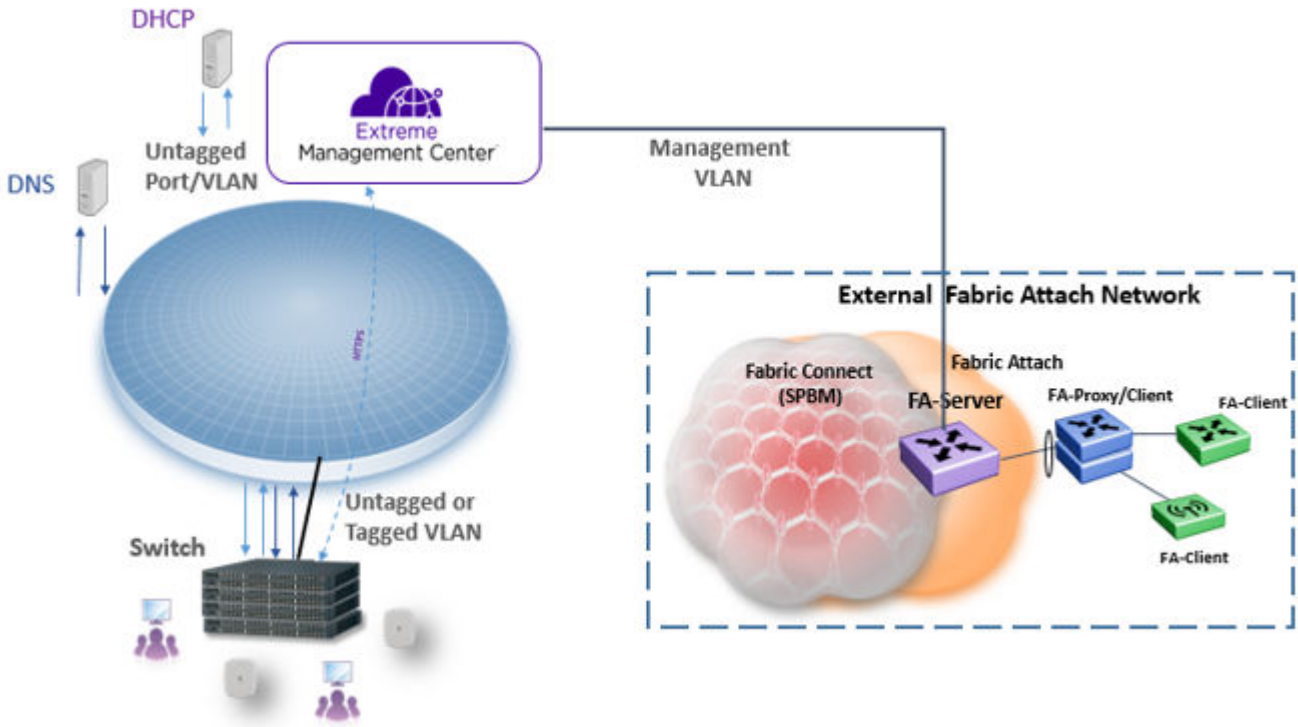
`reset` parameter. Then, use the **`boot`** command to restore the switch (or stack) to factory default settings after the reboot.

- 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 cli password
      ```

    - 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 is 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:R0D.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:R0D.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.
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

             Status
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 cli password
Access Login     Username / Password
------ --------- ----------------------------------
RW     RW        ztp-admin / ***************
RO     RO        RO / ***************
```

- 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
```