



Interface and Hardware Components Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst 9400 Switches)

First Published: 2017-07-31

Last Modified: 2017-11-03

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

Configuring Interface Characteristics 1

Finding Feature Information 1

Information About Interface Characteristics 1

Interface Types 1

Port-Based VLANs 1

Switch Ports 2

Using the Switch USB Ports 5

USB Mini-Type B Console Port 5

Console Port Change Logs 5

USB Type A Port 6

USB 2.0 Host Port 6

Interface Connections 6

Interface Configuration Mode 7

Default Ethernet Interface Configuration 7

Interface Speed and Duplex Mode 8

Speed and Duplex Configuration Guidelines 9

IEEE 802.3x Flow Control 9

Layer 3 Interfaces 10

How to Configure Interface Characteristics 11

Configuring Interfaces 11

Adding a Description for an Interface 12

Configuring a Range of Interfaces 13

Configuring and Using Interface Range Macros 14

Configuring Ethernet Interfaces 16

Setting the Interface Speed and Duplex Parameters 16

Configuring Forty Gigabit Ethernet Interface 17

Configuring IEEE 802.3x Flow Control	18
Configuring Layer 3 Interfaces	19
Configuring a Logical Layer 3 GRE Tunnel Interface	20
Configuring SVI Autostate Exclude	21
Shutting Down and Restarting the Interface	22
Configuring USB Inactivity Timeout	23
Monitoring Interface Characteristics	24
Monitoring Interface Status	24
Clearing and Resetting Interfaces and Counters	25
Configuration Examples for Interface Characteristics	26
Adding a Description to an Interface: Example	26
Configuring a Range of Interfaces: Examples	26
Configuring and Using Interface Range Macros: Examples	26
Setting Interface Speed and Duplex Mode: Example	26
Configuring Layer 3 Interfaces: Example	27
Example: Configuring the USB Inactivity Timeout	27
Feature History for Configuring Interface Characteristics	27

CHAPTER 2
Configuring Auto-MDIX 29

Prerequisites for Auto-MDIX	29
Restrictions for Auto-MDIX	29
Information About Configuring Auto-MDIX	29
Auto-MDIX on an Interface	29
How to Configure Auto-MDIX	30
Configuring Auto-MDIX on an Interface	30
Example for Configuring Auto-MDIX	31
Auto-MDIX and Operational State	31
Additional References for Auto-MDIX	32
Feature History for Auto-MDIX	32

CHAPTER 3
Configuring Ethernet Management Port 33

Prerequisites for Ethernet Management Ports	33
Information About the Ethernet Management Port	33
Ethernet Management Port Direct Connection to a Device	34

Ethernet Management Port and Routing	34
Supported Features on the Ethernet Management Port	34
How to Configure the Ethernet Management Port	35
Disabling and Enabling the Ethernet Management Port	35
Example for Configuring IP Address on Ethernet Management Interface	36
Additional References for Ethernet Management Ports	37
Feature History for Ethernet Management Port	37

CHAPTER 4

Checking Port Status and Connectivity 39

Check Connected Modules	39
Checking Interface Status	40
Displaying MAC Addresses	41
Checking Cable Status Using Time Domain Reflectometer	42
Running the TDR Test	42
TDR Guidelines	42
Using Telnet	43
Changing the Logout Timer	43
Monitoring User Sessions	44
Using Ping	45
Understanding How Ping Works	45
Running Ping	45
Using IP Traceroute	46
Understanding How IP Traceroute Works	46
Running IP Traceroute	46
Using Layer 2 Traceroute	47
Layer 2 Traceroute Usage Guidelines	47
Running Layer 2 Traceroute	48
Configuring ICMP	49
Enabling ICMP Protocol Unreachable Messages	49
Enabling ICMP Mask Reply Messages	49
Feature History for Checking Port Status and Connectivity	50

CHAPTER 5

Configuring LLDP, LLDP-MED, and Wired Location Service 51

Restrictions for LLDP	51
-----------------------	----

Information About LLDP, LLDP-MED, and Wired Location Service	51
LLDP	51
LLDP Supported TLVs	52
LLDP-MED	52
LLDP-MED Supported TLVs	52
Wired Location Service	54
Default LLDP Configuration	55
How to Configure LLDP, LLDP-MED, and Wired Location Service	55
Enabling LLDP	55
Configuring LLDP Characteristics	56
Configuring LLDP-MED TLVs	58
Configuring Network-Policy TLV	59
Configuring Location TLV and Wired Location Service	61
Enabling Wired Location Service on the Device	64
Configuration Examples for LLDP, LLDP-MED, and Wired Location Service	65
Configuring Network-Policy TLV: Examples	65
Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service	65
Additional References for LLDP, LLDP-MED, and Wired Location Service	66
Feature History for LLDP, LLDP-MED, and Wired Location Service	67

CHAPTER 6

Configuring System MTU	69
Restrictions for System MTU	69
Information About the MTU	69
System MTU Value Application	69
How to Configure MTU	70
Configuring the System MTU	70
Configuring Protocol-Specific MTU	70
Configuration Examples for System MTU	71
Example: Configuring Protocol-Specific MTU	71
Example: Configuring the System MTU	71
Additional References for System MTU	72
Feature History for System MTU	72

CHAPTER 7

Configuring COAP Proxy Server	73
--------------------------------------	-----------

Restrictions for the COAP Proxy Server	73
Information About the COAP Proxy Server	73
How to Configure the COAP Proxy Server	74
Configuring the COAP Proxy	74
Configuring COAP Endpoints	76
Configuration Examples for the COAP Proxy Server	77
Examples: Configuring the COAP Proxy Server	77
Monitoring COAP Proxy Server	81
Feature Information for COAP	82

CHAPTER 8

Configuring 2-event Classification 83

Restrictions for 2-event classification	83
Information about 2-event Classification	83
Configuring 2-event Classification	83
Example: Configuring 2-Event Classification	84
Feature Information for 2-event Classification	84

CHAPTER 9

Configuring PoE 87

Information About PoE	87
PoE and PoE+ Ports	87
Supported Protocols and Standards	87
Powered-Device Detection and Initial Power Allocation	88
Power Management Modes	89
Cisco Universal Power Over Ethernet	91
How to Configure PoE and UPoE	92
Configuring a Power Management Mode on a PoE Port	92
Enabling Power on Signal/Spare Pairs	94
Configuring Power Policing	94
Monitoring Power Status	96
Additional References for PoE	97
Feature History for Power over Ethernet	97

CHAPTER 10

Configuring EEE 99

Restrictions for EEE	99
----------------------	----

Information About EEE	99
EEE Overview	99
Default EEE Configuration	100
How to Configure EEE	100
Enabling or Disabling EEE	100
Monitoring EEE	101
Configuration Examples for Configuring EEE	101
Additional References for EEE	102
Feature History for Configuring EEE	102

CHAPTER 11

M2 SATA Module on Cisco Catalyst 9400 Series Supervisor	105
M2 SATA Module on Cisco Catalyst 9400 Series Supervisor	105
File System and Storage on M2 SATA	105
Accessing File System on M2 SATA	106
Formatting the M2 SATA Flash Disk	106
Operations on the SATA Module	106
Feature History and Information for M2 SATA Module	107



CHAPTER 1

Configuring Interface Characteristics

- [Finding Feature Information, on page 1](#)
- [Information About Interface Characteristics, on page 1](#)
- [How to Configure Interface Characteristics, on page 11](#)
- [Setting Interface Speed and Duplex Mode: Example, on page 26](#)
- [Configuring Layer 3 Interfaces: Example, on page 27](#)
- [Example: Configuring the USB Inactivity Timeout, on page 27](#)
- [Feature History for Configuring Interface Characteristics, on page 27](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Information About Interface Characteristics

The following sections provide information about interface characteristics.

Interface Types

This section describes the different types of interfaces supported by the device. The rest of the chapter describes configuration procedures for physical interface characteristics.

Port-Based VLANs

A VLAN is a switched network that is logically segmented by function, team, or application, without regard to the physical location of the users. Packets received on a port are forwarded only to ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLANs.

VLAN partitions provide hard firewalls for traffic in the VLAN, and each VLAN has its own MAC address table. A VLAN comes into existence when a local port is configured to be associated with the VLAN, when the VLAN Trunking Protocol (VTP) learns of its existence from a neighbor on a trunk, or when a user creates a VLAN.

To configure VLANs, use the **vlan** *vlan-id* global configuration command to enter VLAN configuration mode. The VLAN configurations for normal-range VLANs (VLAN IDs 1 to 1005) are saved in the VLAN database. If VTP is version 1 or 2, to configure extended-range VLANs (VLAN IDs 1006 to 4094), you must first set VTP mode to transparent. Extended-range VLANs created in transparent mode are not added to the VLAN database but are saved in the device running configuration. With VTP version 3, you can create extended-range VLANs in client or server mode in addition to transparent mode. These VLANs are saved in the VLAN database.

Add ports to a VLAN by using the **switchport** command in interface configuration mode.

- Identify the interface.
- For a trunk port, set trunk characteristics, and, if desired, define the VLANs to which it can belong.
- For an access port, set and define the VLAN to which it belongs.

Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. Switch ports belong to one or more VLANs. A switch port can be an access port or a trunk port. You can configure a port as an access port or trunk port or let the Dynamic Trunking Protocol (DTP) operate on a per-port basis to set the switchport mode by negotiating with the port on the other end of the link. switch ports are used for managing the physical interface and associated Layer 2 protocols and do not handle routing or bridging.

Configure switch ports by using the **switchport** interface configuration commands.

Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives a tagged packet (Inter-Switch Link [ISL] or IEEE 802.1Q tagged), the packet is dropped, and the source address is not learned.

The types of access ports supported are:

- Static access ports are manually assigned to a VLAN (or through a RADIUS server for use with IEEE 802.1x).

You can also configure an access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.

Trunk Ports

A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. These trunk port types are supported:

- In an ISL trunk port, all received packets are expected to be encapsulated with an ISL header, and all transmitted packets are sent with an ISL header. Native (non-tagged) frames received from an ISL trunk port are dropped.
- An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An IEEE 802.1Q trunk port is assigned a default port VLAN ID (PVID), and all untagged traffic travels on the port default

PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Although by default, a trunk port is a member of every VLAN known to the VTP, you can limit VLAN membership by configuring an allowed list of VLANs for each trunk port. The list of allowed VLANs does not affect any other port but the associated trunk port. By default, all possible VLANs (VLAN ID 1 to 4094) are in the allowed list. A trunk port can become a member of a VLAN only if VTP knows of the VLAN and if the VLAN is in the enabled state. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of that VLAN and traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of a new, enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and no traffic for the VLAN is forwarded to or from the port.

Tunnel Ports

Tunnel ports are used in IEEE 802.1Q tunneling to segregate the traffic of customers in a service-provider network from other customers who are using the same VLAN number. You configure an asymmetric link from a tunnel port on a service-provider edge switch to an IEEE 802.1Q trunk port on the customer switch. Packets entering the tunnel port on the edge switch, already IEEE 802.1Q-tagged with the customer VLANs, are encapsulated with another layer of an IEEE 802.1Q tag (called the metro tag), containing a VLAN ID unique in the service-provider network, for each customer. The double-tagged packets go through the service-provider network keeping the original customer VLANs separate from those of other customers. At the outbound interface, also a tunnel port, the metro tag is removed, and the original VLAN numbers from the customer network are retrieved.

Tunnel ports cannot be trunk ports or access ports and must belong to a VLAN unique to each customer.

Routed Ports

A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as DTP and STP.

Configure routed ports by putting the interface into Layer 3 mode with the **no switchport** interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the **ip routing** and **router protocol** global configuration commands.



Note Entering a **no switchport** interface configuration command shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost.

The number of routed ports that you can configure is not limited by software. However, the interrelationship between this number and the number of other features being configured might impact CPU performance because of hardware limitations.



Note The Network Essentials license supports static routing and the Routing Information Protocol (RIP). For full Layer 3 routing, you must enable the Network Advantage license on the standalone device, or the active device, or the standby device.

Switch Virtual Interfaces

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing function in the system. You can associate only one SVI with a VLAN. You configure an SVI for a VLAN only to route between VLANs or to provide IP host connectivity to the device. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote device administration. Additional SVIs must be explicitly configured.



Note You cannot delete interface VLAN 1.

SVIs provide IP host connectivity only to the system. SVIs are created the first time that you enter the **vlan** interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an ISL or IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address.

You can also use the interface range command to configure existing VLAN SVIs within the range. The commands entered under the interface range command are applied to all existing VLAN SVIs within the range. You can enter the command **interface range create vlan** *x - y* to create all VLANs in the specified range that do not already exist. When the VLAN interface is created, **interface range vlan** *id* can be used to configure the VLAN interface.

Although the device supports a total of 1005 VLANs and SVIs, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might impact CPU performance because of hardware limitations.

When you create an SVI, it does not become active until it is associated with a physical port.

EtherChannel Port Groups

EtherChannel port groups treat multiple switch ports as one switch port. These port groups act as a single logical port for high-bandwidth connections between devices or between devices and servers. An EtherChannel balances the traffic load across the links in the channel. If a link within the EtherChannel fails, traffic previously carried over the failed link changes to the remaining links. You can group multiple trunk ports into one logical trunk port, group multiple access ports into one logical access port, group multiple tunnel ports into one logical tunnel port, or group multiple routed ports into one logical routed port. Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. Exceptions are the DTP, the Cisco Discovery Protocol (CDP), and the Port Aggregation Protocol (PAgP), which operate only on physical ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel. For Layer 3 interfaces, you manually create the logical interface by using the **interface port-channel** global configuration command. Then you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command. For Layer 2 interfaces, use the **channel-group** interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together.

Uplink Ports

The supervisor module has 10 uplink ports, named 1 to 10. The first eight uplink ports, 1 to 8, use Small Form-Factor Pluggable (SFP) transceivers or SFP+ transceivers and uplink ports 9 and 10 use Quad Small Form-Factor Pluggable (QSFP) transceivers. Ports 1 to 8 are 10-Gigabit Ethernet ports that support both 10G and 1G transceivers. Ports 9 and 10 are the QSFP ports that support 40 Gigabit Ethernet uplinks.

By default the 10-Gigabit Ethernet ports 1 to 8 are enabled.

40-Gigabit Ethernet Port 9 can be enabled only when ports 1 to 4 are enabled. 40-Gigabit Ethernet Port 10 can be enabled only when ports 5 to 9 are enabled.

Power over Ethernet

The Power over Ethernet (PoE) technology allows PoE (802.3af standard), PoE+ (802.3at) ports to supply power for the operation of a device.

Cisco Universal Power Over Ethernet (Cisco UPoE) extends the IEEE PoE+ standard to double the power per port to 60 watts.

For more information, see the *Configuring PoE* section of this guide

Using the Switch USB Ports

The device has two USB ports on the front panel — a USB mini-Type B console port and a USB Type A port.

USB Mini-Type B Console Port

The device has the following console ports:

- USB mini-Type B console connection
- RJ-45 console port

Console output appears on devices connected to both ports, but console input is active on only one port at a time. By default, the USB connector takes precedence over the RJ-45 connector.

**Note**

Windows PCs require a driver for the USB port. See the hardware installation guide for driver installation instructions.

Use the supplied USB Type A-to-USB mini-Type B cable to connect a PC or other device to the device. The connected device must include a terminal emulation application. When the device detects a valid USB connection to a powered-on device that supports host functionality (such as a PC), input from the RJ-45 console is immediately disabled, and input from the USB console is enabled. Removing the USB connection immediately reenables input from the RJ-45 console connection. An LED on the device shows which console connection is in use.

Console Port Change Logs

At software startup, a log shows whether the USB or the RJ-45 console is active. Every device always first displays the RJ-45 media type.

In the sample output, Device 1 has a connected USB console cable. Because the bootloader did not change to the USB console, the first log from Device 1 shows the RJ-45 console. A short time later, the console changes and the USB console log appears. Device 2 and Device 3 have connected RJ-45 console cables.

When the USB cable is removed or the PC de-activates the USB connection, the hardware automatically changes to the RJ-45 console interface:

You can configure the console type to always be RJ-45, and you can configure an inactivity timeout for the USB connector.

USB Type A Port

The USB Type A port provides access to external USB flash devices, also known as thumb drives or USB keys. The port supports Cisco USB flash drives, USB 2.0 and USB 3.0, with capacities from 128 MB to 8 GB (USB devices with port densities of 128 MB, 256 MB, 1 GB, 4 GB, 8 GB are supported). USB 3.0 is also called SuperSpeed USB, used for higher file transfer rates. You can use standard Cisco IOS command-line interface (CLI) commands to read, write, erase, and copy to or from the flash device. You can also configure the device to boot from the USB flash drive.

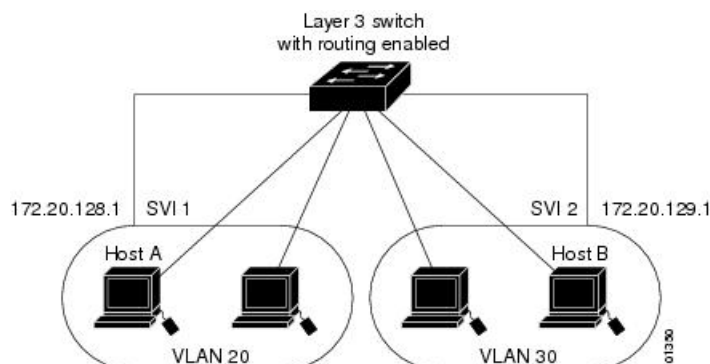
USB 2.0 Host Port

The USB 2.0 host port provides access to external USB flash devices, also known as thumb drives or USB keys. The port supports Cisco USB flash drives with capacities from 128 MB to 8 GB (USB devices with port densities of 128 MB, 256 MB, 1 GB, 4 GB, 8 GB are supported). You can use standard Cisco IOS command-line interface (CLI) commands to read, write, erase, and copy to or from the flash device. You can also configure the device to boot from the USB flash drive.

Interface Connections

Devices within a single VLAN can communicate directly through any switch. Ports in different VLANs cannot exchange data without going through a routing device. With a standard Layer 2 device, ports in different VLANs have to exchange information through a router. By using the device with routing enabled, when you configure both VLAN 20 and VLAN 30 with an SVI to which an IP address is assigned, packets can be sent from Host A to Host B directly through the device with no need for an external router.

Figure 1: Connecting VLANs with the Switch



When the Network Advantage license is used on the device or the active device, the device uses the routing method to forward traffic between interfaces. If the Network Essentials license is used on the device or the active device, only basic routing (static routing and RIP) is supported. Whenever possible, to maintain high

performance, forwarding is done by the device hardware. However, only IPv4 packets with Ethernet II encapsulation are routed in hardware.

The routing function can be enabled on all SVIs and routed ports. The device routes only IP traffic. When IP routing protocol parameters and address configuration are added to an SVI or routed port, any IP traffic received from these ports is routed.

Interface Configuration Mode

The device supports these interface types:

- Physical ports—device ports and routed ports
- VLANs—switch virtual interfaces
- Port channels—EtherChannel interfaces

You can also configure a range of interfaces.

To configure a physical interface (port), specify the interface type, module number, and device port number, and enter interface configuration mode.

-
- Module number—The module or slot number on the device: switch (downlink) ports are 0, and uplink ports are 1.
- On a device with SFP uplink ports, the module number is 1 and the port numbers restart. For example, if the device has 24 10/100/1000 ports, the SFP module ports are gigabitethernet1/1/1 through gigabitethernet1/1/4 or tengigabitethernet1/1/1 through tengigabitethernet1/1/4.

You can identify physical interfaces by physically checking the interface location on the device. You can also use the **show** privileged EXEC commands to display information about a specific interface or all the interfaces on the switch. The remainder of this chapter primarily provides physical interface configuration procedures.

These are examples of how to identify interfaces on standalone devices:

Default Ethernet Interface Configuration

To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the **switchport** interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

This table shows the Ethernet interface default configuration, including some features that apply only to Layer 2 interfaces.

Table 1: Default Layer 2 Ethernet Interface Configuration

Feature	Default Setting
Operating mode	Layer 2 or switching mode (switchport command).
Allowed VLAN range	VLANs 1 to 4094.

Feature	Default Setting
Default VLAN (for access ports)	VLAN 1 (Layer 2 interfaces only).
Native VLAN (for IEEE 802.1Q trunks)	VLAN 1 (Layer 2 interfaces only).
VLAN trunking	Switchport mode dynamic auto (supports DTP) (Layer 2 interfaces only).
Port enable state	All ports are enabled.
Port description	None defined.
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
Flow control	Flow control is set to receive: off . It is always off for sent packets.
EtherChannel (PAgP)	Disabled on all Ethernet ports.
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked) (Layer 2 interfaces only).
Broadcast, multicast, and unicast storm control	Disabled.
Protected port	Disabled (Layer 2 interfaces only).
Port security	Disabled (Layer 2 interfaces only).
Port Fast	Disabled.
Auto-MDIX	Enabled. Note The switch might not support a pre-standard powered device, such as Cisco IP phones and access points that do not fully support IEEE 802.3af, if that powered device is connected to the switch through a crossover cable. This is regardless of whether auto-MDIX is enabled on the switch port.
Power over Ethernet (PoE)	Enabled (auto).

Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, 1000 Mb/s and in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mb/s ports operate in half-duplex mode, which means that stations can either receive or send traffic.

Switch modules include Gigabit Ethernet (10/100/1000-Mb/s) ports, SFP+ modules, and small form-factor pluggable (SFP) module slots supporting SFP modules.

Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- Do not disable Auto-Negotiation on PoE switches.
- Gigabit Ethernet (10/100/1000-Mb/s) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mb/s do not support half-duplex mode.
- For SFP module ports, the speed and duplex CLI options change depending on the SFP module type:
 - The 1000BASE-*x* (where *x* is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the **nonegotiate** keyword in the **speed** interface configuration command. Duplex options are not supported.
 - The 1000BASE-T SFP module ports support the same speed and duplex options as the 10/100/1000-Mb/s ports.
- If both ends of the line support autonegotiation, we highly recommend the default setting of **auto** negotiation.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- When STP is enabled and a port is reconfigured, the device can take up to 30 seconds to check for loops. The port LED is amber while STP reconfigures. As best practice, we suggest configuring the speed and duplex options on a link to auto or to fixed on both the ends. If one side of the link is configured to auto and the other side is configured to fixed, the link will not be up and this is expected.
- As best practice, we suggest configuring the speed and duplex options on a link to auto or to fixed on both the ends. If one side of the link is configured to auto and the other side is configured to fixed, the link will not be up and this is expected.

**Caution**

Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

IEEE 802.3x Flow Control

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

**Note**

The switch ports can receive, but not send, pause frames.

You use the **flowcontrol** interface configuration command to set the interface's ability to **receive** pause frames to **on**, **off**, or **desired**. Prior to Cisco IOS XE Everest 16.6.4 release, the default state is **off**. Starting Cisco IOS XE Everest 16.6.4 release, the default state is **on**.

When set to **desired**, an interface can operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.

These rules apply to flow control settings on the device:

- **receive on** (or **desired**): The port cannot send pause frames but can operate with an attached device that is required to or can send pause frames; the port can receive pause frames.
- **receive off**: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

**Note**

For details on the command settings and the resulting flow control resolution on local and remote ports, see the **flowcontrol** interface configuration command in the command reference for this release.

Layer 3 Interfaces

The device supports these types of Layer 3 interfaces:

- **SVIs**: You should configure SVIs for any VLANs for which you want to route traffic. SVIs are created when you enter a VLAN ID following the **interface vlan** global configuration command. To delete an SVI, use the **no interface vlan** global configuration command. You cannot delete interface VLAN 1.

**Note**

When you create an SVI, it does not become active until it is associated with a physical port.

When configuring SVIs, you can use the **switchport autostate exclude** command on a port to exclude that port from being included in determining SVI line-state. To disable autostate on the SVI, use the **no autostate** command on the SVI.

- **Routed ports**: Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command.
- **Layer 3 EtherChannel ports**: EtherChannel interfaces made up of routed ports.

A Layer 3 device can have an IP address assigned to each routed port and SVI.

There is no defined limit to the number of SVIs and routed ports that can be configured in a device or in a device stack. However, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might have an impact on CPU usage because of hardware limitations. If the device is using its maximum hardware resources, attempts to create a routed port or SVI have these results:

- If you try to create a new routed port, the device generates a message that there are not enough resources to convert the interface to a routed port, and the interface remains as a switchport.
- If you try to create an extended-range VLAN, an error message is generated, and the extended-range VLAN is rejected.
- If the device is notified by VLAN Trunking Protocol (VTP) of a new VLAN, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.

- If the device attempts to boot up with a configuration that has more VLANs and routed ports than hardware can support, the VLANs are created, but the routed ports are shut down, and the device sends a message that this was due to insufficient hardware resources.



Note All Layer 3 interfaces require an IP address to route traffic. This procedure shows how to configure an interface as a Layer 3 interface and how to assign an IP address to an interface:

If the physical port is in Layer 2 mode (the default), you must enter the **no switchport** interface configuration command to put the interface into Layer 3 mode. Entering a **no switchport** command disables and then re-enables the interface, which might generate messages on the device to which the interface is connected. Furthermore, when you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration

How to Configure Interface Characteristics

Configuring Interfaces

These general instructions apply to all interface configuration processes.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface Example:	Identifies the interface type, and the number of the connector. Note You do not need to add a space between the interface type and the interface number.
Step 4	Follow each interface command with the interface configuration commands that the interface requires.	Defines the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you

	Command or Action	Purpose
		enter another interface command or enter end to return to privileged EXEC mode.
Step 5	interface range or interface range macro	(Optional) Configures a range of interfaces. Note Interfaces configured in a range must be the same type and must be configured with the same feature options.
Step 6	show interfaces	Displays a list of all interfaces on or configured for the switch. A report is provided for each interface that the device supports or for the specified interface.

Adding a Description for an Interface

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet1/0/2	Specifies the interface for which you are adding a description, and enter interface configuration mode.
Step 4	description <i>string</i> Example: Device(config-if)# description Connects to Marketing	Adds a description for an interface.

	Command or Action	Purpose
Step 5	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 6	show interfaces <i>interface-id</i> description	Verifies your entry.
Step 7	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring a Range of Interfaces

To configure multiple interfaces with the same configuration parameters, use the **interface range** global configuration command. When you enter the interface-range configuration mode, all command parameters that you enter are attributed to all interfaces within that range until you exit this mode.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface range {<i>port-range</i> <i>macro</i> <i>macro_name</i>} Example: <pre>Device(config)# interface range macro</pre>	Specifies the range of interfaces (VLANs or physical ports) to be configured, and enter interface-range configuration mode. <ul style="list-style-type: none"> • You can use the interface range command to configure up to five port ranges or a previously defined macro. • The macro variable is explained in the section on <i>Configuring and Using Interface Range Macros</i>.

	Command or Action	Purpose
		<ul style="list-style-type: none"> In a comma-separated <i>port-range</i>, you must enter the interface type for each entry and enter spaces before and after the comma. In a hyphen-separated <i>port-range</i>, you do not need to re-enter the interface type, but you must enter a space before the hyphen. <p>Note Use the normal configuration commands to apply the configuration parameters to all interfaces in the range. Each command is executed as it is entered.</p>
Step 4	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show interfaces [<i>interface-id</i>] Example: <pre>Device# show interfaces</pre>	Verifies the configuration of the interfaces in the range.
Step 6	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring and Using Interface Range Macros

You can create an interface range macro to automatically select a range of interfaces for configuration. Before you can use the **macro** keyword in the **interface range macro** global configuration command string, you must use the **define interface-range** global configuration command to define the macro.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	define interface-range <i>macro_name</i> <i>interface-range</i> Example:	Defines the interface-range macro, and save it in NVRAM. <ul style="list-style-type: none"> • The <i>macro_name</i> is a 32-character maximum character string. • A macro can contain up to five comma-separated interface ranges. • Each <i>interface-range</i> must consist of the same port type. <p>Note Before you can use the macro keyword in the interface range macro global configuration command string, you must use the define interface-range global configuration command to define the macro.</p>
Step 4	interface range macro <i>macro_name</i> Example: <pre>Device(config)# interface range macro enet_list</pre>	Selects the interface range to be configured using the values saved in the interface-range macro called <i>macro_name</i> . You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro.
Step 5	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	show running-config include define Example: <pre>Device# show running-config include define</pre>	Shows the defined interface range macro configuration.
Step 7	copy running-config startup-config Example: <pre>Device# copy running-config</pre>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	<code>startup-config</code>	

Configuring Ethernet Interfaces

Setting the Interface Speed and Duplex Parameters

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet1/0/3</pre>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 4	duplex {auto full half} Example: <pre>Device(config-if)# duplex half</pre>	This command is not available on a 10-Gigabit Ethernet interface. Enter the duplex parameter for the interface. Enable half-duplex mode (for interfaces operating only at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 Mb/s. You can configure the duplex setting when the speed is set to auto .
Step 5	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show interfaces <i>interface-id</i> Example: <pre>Device# show interfaces gigabitethernet1/0/3</pre>	Displays the interface speed and duplex mode configuration.
Step 7	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.
Step 8	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring Forty Gigabit Ethernet Interface

Follow these steps to configure the forty gigabit ethernet interface. Use the no form of the command to disable the fortygigabit ethernet interface.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>interfaceid</i> Example: <pre>Device(config)# interface fortygigabitethernet1/0/9 Device(config-if)#</pre>	Specifies the interface type, that has to be configured.

	Command or Action	Purpose
Step 4	enable Example: Device (config-if) # enable	Enables the fortygigabit ethernet interface. Use no enable command to disable the fortygigabit ethernet interface.

Configuring IEEE 802.3x Flow Control

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode
Step 2	interface <i>interface-id</i> Example:	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 3	flowcontrol {receive} {on off desired} Example: Device (config-if) # flowcontrol receive on	Configures the flow control mode for the port.
Step 4	end Example: Device (config-if) # end	Returns to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> Example:	Verifies the interface flow control settings.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring Layer 3 Interfaces

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface {gigabitethernet interface-id} {vlan vlan-id} {port-channel port-channel-number} Example: <pre>Device(config)# interface gigabitethernet1/0/2</pre>	Specifies the interface to be configured as a Layer 3 interface, and enter interface configuration mode.
Step 4	no switchport Example: <pre>Device(config-if)# no switchport</pre>	For physical ports only, enters Layer 3 mode.
Step 5	ip address ip_address subnet_mask Example: <pre>Device(config-if)# ip address 192.20.135.21 255.255.255.0</pre>	Configures the IP address and IP subnet.
Step 6	no shutdown Example: <pre>Device(config-if)# no shutdown</pre>	Enables the interface.
Step 7	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	show interfaces [<i>interface-id</i>]	Verifies the configuration.
Step 9	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring a Logical Layer 3 GRE Tunnel Interface

Before you begin

Generic Routing Encapsulation (GRE) is a tunneling protocol used to encapsulate network layer protocols inside virtual point-to-point links. A GRE tunnel only provides encapsulation and not encryption.



Note

- GRE tunnels are supported on the hardware on Cisco Catalyst 9000 switches. When GRE is configured without tunnel options, packets are hardware-switched. When GRE is configured with tunnel options (such as key, checksum, and so on), packets are switched in the software. A maximum of 1000 GRE tunnels are supported.
- Other features such as Access Control Lists (ACL) and Quality of Service (QoS) are not supported for the GRE tunnels.
- The **tunnel path-mtu-discovery** command is not supported for GRE tunnels. To avoid fragmentation, you can set the maximum transmission unit (MTU) of both ends of the GRE tunnel to the lowest value by using the **ip mtu 256** command.

To configure a GRE tunnel, perform this task:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface tunnel <i>number</i> Example: Device(config)# interface tunnel 2	Enables tunneling on the interface.
Step 4	ip address <i>ip_address</i> <i>subnet_mask</i> Example: Device(config)# ip address 100.1.1.1 255.255.255.0	Configures the IP address and IP subnet.
Step 5	tunnel source { <i>ip_address</i> <i>type_number</i> } Example: Device(config)# tunnel source 10.10.10.1	Configures the tunnel source.
Step 6	tunnel destination { <i>host_name</i> <i>ip_address</i> } Example: Device(config)# tunnel destination 10.10.10.2	Configures the tunnel destination.
Step 7	tunnel mode gre ip Example: Device(config)# tunnel mode gre ip	Configures the tunnel mode.
Step 8	end Example: Device(config)# end	Exits configuration mode.

Configuring SVI Autostate Exclude

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>interface-id</i> Example:	Specifies a Layer 2 interface (physical port or port channel), and enter interface configuration mode.
Step 4	switchport autostate exclude Example: Device (config-if) # switchport autostate exclude	Excludes the access or trunk port when defining the status of an SVI line state (up or down)
Step 5	end Example: Device (config-if) # end	Returns to privileged EXEC mode.
Step 6	show running config interface <i>interface-id</i>	(Optional) Shows the running configuration. Verifies the configuration.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Shutting Down and Restarting the Interface

Shutting down an interface disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface is not mentioned in any routing updates.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface {vlan <i>vlan-id</i> } { gigabitethernet <i>interface-id</i> } { port-channel <i>port-channel-number</i> } Example: Device(config) # interface gigabitethernet1/0/2	Selects the interface to be configured.
Step 4	shutdown Example: Device(config-if) # shutdown	Shuts down an interface.
Step 5	no shutdown Example: Device(config-if) # no shutdown	Restarts an interface.
Step 6	end Example: Device(config-if) # end	Returns to privileged EXEC mode.
Step 7	show running-config Example: Device# show running-config	Verifies your entries.

Configuring USB Inactivity Timeout

The configurable inactivity timeout reactivates the RJ-45 console port if the USB console port is activated but no input activity occurs on it for a specified time period. When the USB console port is deactivated due to a timeout, you can restore its operation by disconnecting and reconnecting the USB cable.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	line console 0 Example: Device(config)# line console 0	Configures the console and enters line configuration mode.
Step 4	usb-inactivity-timeout switch <i>switch_number</i> <i>timeout-minutes</i> Example: Device(config-line)# usb-inactivity-timeout switch 1 30	Specifies an inactivity timeout for the console port. The range is 1 to 240 minutes. The default is to have no timeout configured.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring Interface Characteristics

Monitoring Interface Status

Commands entered at the privileged EXEC prompt display information about the interface, including the versions of the software and the hardware, the configuration, and statistics about the interfaces.

Table 2: Show Commands for Interfaces

Command	Purpose
show interfaces <i>interface-id</i> status [err-disabled]	Displays interface status or a list of interfaces in the error-disabled state.
show interfaces [<i>interface-id</i>] switchport	Displays administrative and operational status of switching (nonrouting) ports. You can use this command to find out if a port is in routing or in switching mode.
show interfaces [<i>interface-id</i>] description	Displays the description configured on an interface or all interfaces and the interface status.

Command	Purpose
show ip interface [<i>interface-id</i>]	Displays the usability status of all interfaces configured for IP routing or the specified interface.
show interface [<i>interface-id</i>] stats	Displays the input and output packets by the switching path for the interface.
show interfaces <i>interface-id</i>	(Optional) Displays speed and duplex on the interface.
show interfaces transceiver dom-supported-list	(Optional) Displays Digital Optical Monitoring (DOM) status on the connect SFP modules.
show interfaces transceiver properties	(Optional) Displays temperature, voltage, or amount of current on the interface.
show interfaces [<i>interface-id</i>] [{ transceiver properties detail }] <i>module number</i>	Displays physical and operational status about an SFP module.
show running-config interface [<i>interface-id</i>]	Displays the running configuration in RAM for the interface.
show version	Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images.
show controllers ethernet-controller <i>interface-id</i> phy	Displays the operational state of the auto-MDIX feature on the interface.

Clearing and Resetting Interfaces and Counters

Table 3: Clear Commands for Interfaces

Command	Purpose
clear counters [<i>interface-id</i>]	Clears interface counters.
clear interface <i>interface-id</i>	Resets the hardware logic on an interface.
clear line [<i>number</i> console 0 vty number]	Resets the hardware logic on an asynchronous serial line.



Note The **clear counters** privileged EXEC command does not clear counters retrieved by using Simple Network Management Protocol (SNMP), but only those seen with the **show interface** privileged EXEC command.

Configuration Examples for Interface Characteristics

Adding a Description to an Interface: Example

Configuring a Range of Interfaces: Examples

If you enter multiple configuration commands while you are in interface-range mode, each command is executed as it is entered. The commands are not batched and executed after you exit interface-range mode. If you exit interface-range configuration mode while the commands are being executed, some commands might not be executed on all interfaces in the range. Wait until the command prompt reappears before exiting interface-range configuration mode.

Configuring and Using Interface Range Macros: Examples

This example shows how to define an interface-range named *enet_list* to include ports 1 and 2 on switch 1 and to verify the macro configuration:

This example shows how to enter interface-range configuration mode for the interface-range macro *enet_list*:

```
Device# configure terminal
Device(config)# interface range macro enet_list
Device(config-if-range)#
```

This example shows how to delete the interface-range macro *enet_list* and to verify that it was deleted.

```
Device# configure terminal
Device(config)# no define interface-range enet_list
Device(config)# end
Device# show run | include define
Device#
```

Setting Interface Speed and Duplex Mode: Example

This example shows how to set the interface speed to 100 Mb/s and the duplex mode to half on a 10/100/1000 Mb/s port:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# speed 10
Device(config-if)# duplex half
```

This example shows how to set the interface speed to 100 Mb/s on a 10/100/1000 Mb/s port:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# speed 100
```

Configuring Layer 3 Interfaces: Example

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)# ip address 192.20.135.21 255.255.255.0
Device(config-if)# no shutdown
```

Example: Configuring the USB Inactivity Timeout

The following example shows how to configure the inactivity timeout to 30 minutes:

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# usb-inactivity-timeout switch 1 30
```

The following example shows how to disable the configuration:

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# no usb-inactivity-timeout switch 1
```

If there is no (input) activity on a USB console port for the configured number of minutes, the inactivity timeout setting applies to the RJ-45 port, and a log shows this occurrence:

```
*Mar  1 00:47:25.625: %USB_CONSOLE-6-INACTIVITY_DISABLE: Console media-type USB disabled
due to inactivity, media-type reverted to RJ45.
```

At this point, the only way to reactivate the USB console port is to disconnect and reconnect the cable.

When the USB cable on the switch has been disconnected and reconnected, a log similar to this appears:

```
*Mar  1 00:48:28.640: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

Feature History for Configuring Interface Characteristics

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.6.1	Interface Characteristics	Interface Characteristics includes interface types, connections, configuration modes, speed, and other aspects of configuring a physical interface on a device.
Cisco IOS XE Everest 16.6.4	IEEE 802.3x Flow Control	The default value for flowcontrol interface configuration command was modified to on on all the models of the series.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 2

Configuring Auto-MDIX

- [Prerequisites for Auto-MDIX, on page 29](#)
- [Restrictions for Auto-MDIX, on page 29](#)
- [Information About Configuring Auto-MDIX, on page 29](#)
- [How to Configure Auto-MDIX, on page 30](#)
- [Example for Configuring Auto-MDIX, on page 31](#)
- [Auto-MDIX and Operational State, on page 31](#)
- [Additional References for Auto-MDIX, on page 32](#)
- [Feature History for Auto-MDIX, on page 32](#)

Prerequisites for Auto-MDIX

To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the **switchport** interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

Automatic medium-dependent interface crossover (auto-MDIX) is enabled by default.

Restrictions for Auto-MDIX

The device might not support a pre-standard powered device—such as Cisco IP phones and access points that do not fully support IEEE 802.3af—if that powered device is connected to the device through a crossover cable. This is regardless of whether auto-MIDX is enabled on the switch port.

Information About Configuring Auto-MDIX

Auto-MDIX on an Interface

When automatic medium-dependent interface crossover (auto-MDIX) is enabled on an interface, the interface automatically detects the required cable connection type (straight through or crossover) and configures the

connection appropriately. When connecting devices without the auto-MDIX feature, you must use straight-through cables to connect to devices such as servers, workstations, or routers and crossover cables to connect to other devices or repeaters. With auto-MDIX enabled, you can use either type of cable to connect to other devices, and the interface automatically corrects for any incorrect cabling. For more information about cabling requirements, see the hardware installation guide.

This table shows the link states that result from auto-MDIX settings and correct and incorrect cabling.

Table 4: Link Conditions and Auto-MDIX Settings

Local Side Auto-MDIX	Remote Side Auto-MDIX	With Correct Cabling	With Incorrect Cabling
On	On	Link up	Link up
On	Off	Link up	Link up
Off	On	Link up	Link up
Off	Off	Link up	Link down

How to Configure Auto-MDIX

Configuring Auto-MDIX on an Interface

Auto MDIX is turned on by default. To disable Auto MDIX on a port, use the **no mdix auto** command under the interface configuration mode. To put it back to default, use the **mdix auto** command in the interface configuration mode. The following steps show how to enable the Auto MDIX.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode
Step 3	interface interface-id Example: Device (config)# interface	Specifies the physical interface to be configured, and enter interface configuration mode.

	Command or Action	Purpose
	<code>gigabitethernet1/0/1</code>	
Step 4	mdix auto Example: <code>Device(config-if)# mdix auto</code>	Enables the Auto MDIX feature.
Step 5	end Example: <code>Device(config-if)# end</code>	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: <code>Device# copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Example for Configuring Auto-MDIX

This example shows how to enable auto-MDIX on a port:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# mdix auto
Device(config-if)# end
```

Auto-MDIX and Operational State

Table 5: Auto-MDIX and Operational State

Auto-MDIX Setting and Operational State on an Interface	Description
Auto-MDIX on (operational: on)	Auto-MDIX is enabled and is fully functioning.
Auto-MDIX on (operational: off)	Auto-MDIX is enabled on this interface but it is not functioning. To allow auto-MDIX feature to function properly, you must also set the interface speed to be autonegotiated.
Auto-MDIX off	Auto-MDIX has been disabled with the no mdix auto command.

Additional References for Auto-MDIX

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for Auto-MDIX

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.6.1	Auto-MDIX on an Interface	An automatic medium-dependent interface crossover (Auto-MDIX) enabled interface detects the required cable connection type (straight through or crossover) and configures the connection appropriately.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 3

Configuring Ethernet Management Port

- [Prerequisites for Ethernet Management Ports, on page 33](#)
- [Information About the Ethernet Management Port, on page 33](#)
- [How to Configure the Ethernet Management Port, on page 35](#)
- [Example for Configuring IP Address on Ethernet Management Interface, on page 36](#)
- [Additional References for Ethernet Management Ports, on page 37](#)
- [Feature History for Ethernet Management Port, on page 37](#)

Prerequisites for Ethernet Management Ports

When connecting a PC to the Ethernet management port, you must first assign an IP address.

Information About the Ethernet Management Port

The Ethernet management port, also referred to as the *Gi0/0* or *GigabitEthernet0/0* port, is a VRF (VPN routing/forwarding) interface to which you can connect a PC. You can use the Ethernet management port instead of the device console port for network management.

When managing a switch, connect the PC to the Ethernet Management port on Catalyst9400 Series Switch.



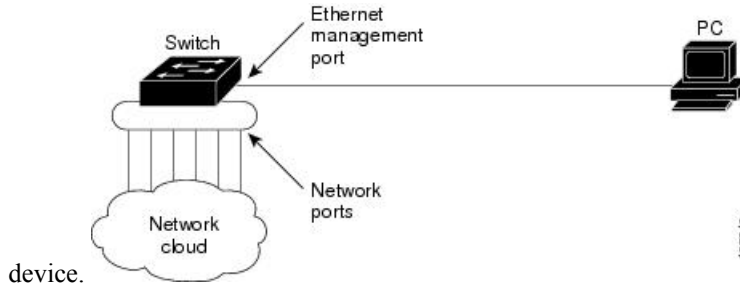
Note

When connecting a PC to the Ethernet management port, you must assign an IP address.

Ethernet Management Port Direct Connection to a Device

Figure 2: Connecting a Switch to a PC

This figure displays how to connect the Ethernet management port to the PC for a device or a standalone

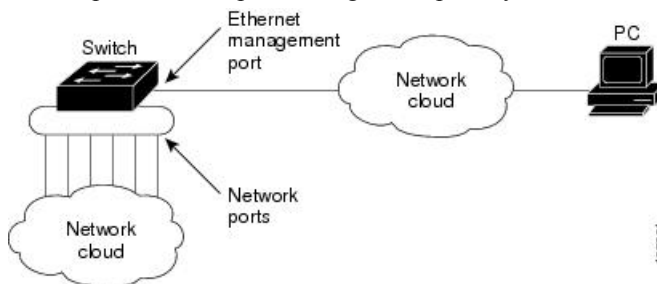


Ethernet Management Port and Routing

By default, the Ethernet management port is enabled. The device cannot route packets from the Ethernet management port to a network port, and the reverse. Even though the Ethernet management port does not support routing, you may need to enable routing protocols on the port.

Figure 3: Network Example with Routing Protocols Enabled

Enable routing protocols on the Ethernet management port when the PC is multiple hops away from the device and the packets must pass through multiple Layer 3 devices to reach the PC.



In the above figure, if the Ethernet management port and the network ports are associated with the same routing process, the routes are propagated as follows:

- The routes from the Ethernet management port are propagated through the network ports to the network.
- The routes from the network ports are propagated through the Ethernet management port to the network.

Because routing is not supported between the Ethernet management port and the network ports, traffic between these ports cannot be sent or received. If this happens, data packet loops occur between the ports, which disrupt the device and network operation. To prevent the loops, configure route filters to avoid routes between the Ethernet management port and the network ports.

Supported Features on the Ethernet Management Port

The Ethernet management port supports these features:

- Express Setup (only in switch stacks)

- Network Assistant
- Telnet with passwords
- TFTP
- Secure Shell (SSH)
- DHCP-based autoconfiguration
- SNMP (only the ENTITY-MIB and the IF-MIB)
- IP ping
- Interface features
 - Speed—10 Mb/s, 100 Mb/s, and autonegotiation
 - Duplex mode—Full, half, and autonegotiation
 - Loopback detection
- Cisco Discovery Protocol (CDP)
- DHCP relay agent
- IPv4 and IPv6 access control lists (ACLs)
- Routing protocols

**Caution**

Before enabling a feature on the Ethernet management port, make sure that the feature is supported. If you try to configure an unsupported feature on the Ethernet Management port, the feature might not work properly, and the device might fail.

How to Configure the Ethernet Management Port

Disabling and Enabling the Ethernet Management Port

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface gigabitethernet0/0 Example: Device(config)# interface gigabitethernet0/0	Specifies the Ethernet management port in the CLI.

	Command or Action	Purpose
Step 3	shutdown Example: Device(config-if) # shutdown	Disables the Ethernet management port.
Step 4	no shutdown Example: Device(config-if) # no shutdown	Enables the Ethernet management port.
Step 5	exit Example: Device(config-if) # exit	Exits interface configuration mode.
Step 6	show interfaces gigabitethernet0/0 Example: Device# show interfaces gigabitethernet0/0	Displays the link status. To find out the link status to the PC, you can monitor the LED for the Ethernet management port. The LED is green (on) when the link is active, and the LED is off when the link is down. The LED is amber when there is a POST failure.

What to do next

Proceed to manage or configure your switch using the Ethernet management port. See the Network Management section.

Example for Configuring IP Address on Ethernet Management Interface

This example shows how to configure IP address on the management interface.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# vrf forwarding Mgmt-vrf
Switch(config-if)# ip address 192.168.247.10 255.255.0.0
Switch(config-if)# end
```

```
Switch# show running-config interface Gi0/0
Building configuration...
```

```
Current configuration : 118 bytes
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
ip address 192.168.247.10 255.255.0.0
negotiation auto
end
```

Additional References for Ethernet Management Ports

Related Documents

Related Topic	Document Title
Bootloader configuration	See the <i>System Management</i> section of this guide.
Bootloader commands	See the <i>System Management Commands</i> section of the <i>Command Reference (Catalyst 9400 Series Switches)</i>

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for Ethernet Management Port

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.6.1	Ethernet Management Port	The Ethernet management port is a VRF interface to which you can connect a PC. You can use the Ethernet management port instead of the device console port for network management.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 4

Checking Port Status and Connectivity

- [Check Connected Modules, on page 39](#)
- [Checking Interface Status, on page 40](#)
- [Displaying MAC Addresses, on page 41](#)
- [Checking Cable Status Using Time Domain Reflectometer, on page 42](#)
- [Using Telnet, on page 43](#)
- [Changing the Logout Timer, on page 43](#)
- [Monitoring User Sessions, on page 44](#)
- [Using Ping, on page 45](#)
- [Using IP Traceroute, on page 46](#)
- [Using Layer 2 Traceroute, on page 47](#)
- [Configuring ICMP, on page 49](#)
- [Feature History for Checking Port Status and Connectivity, on page 50](#)

Check Connected Modules

The Catalyst 9400 series switch is a modular system. You can see which modules are installed, and the MAC address ranges and version numbers for each module, by entering the show module command. Use the *mod_num* argument to specify a particular module number and display detailed information on that module.

This example shows how to check the status for all modules on your switch:

```
Device# show module
```

```
Chassis Type: C9410R
```

Mod	Ports	Card Type	Model	Serial No.
1	48	48-Port UPOE w/ 24p mGig 24p RJ-45	C9400-LC-48UX	JAE2229053D
2	48	48-Port 5Gig/mGig 90W BT (RJ-45)	C9400-LC-48HN	JAE24530BF3
3	48	48-Port UPOE w/ 24p mGig 24p RJ-45	C9400-LC-48UX	JAE2128068Z
4	48	48-Port 5Gig/mGig 90W BT (RJ-45)	C9400-LC-48HN	JAE24241WAY
5	11	Supervisor 1 Module	C9400-SUP-1	JAE22280PL8
6	11	Supervisor 1 Module	C9400-SUP-1	JAE22280PHT
7	48	48-Port UPOE w/ 24p mGig 24p RJ-45	C9400-LC-48UX	JAE2229055N
8	48	48-Port UPOE w/ 24p mGig 24p RJ-45	C9400-LC-48UX	JAE22280DBU
9	48	48-Port UPOE w/ 24p mGig 24p RJ-45	C9400-LC-48UX	JAE22080BWS
10	48	48-Port UPOE w/ 24p mGig 24p RJ-45	C9400-LC-48UX	JAE230707YP
Mod MAC addresses		Hw Fw	Sw	Status

```

1  BC26.C7A4.E738 to BC26.C7A4.E767 1.0 17.5.1r 17.05.01 ok
2  ECCE.13E2.B670 to ECCE.13E2.B69F 1.0 17.5.1r 17.05.01 ok
3  E4AA.5D59.A868 to E4AA.5D59.A897 1.0 17.5.1r 17.05.01 ok
4  A0B4.3982.43C0 to A0B4.3982.43EF 1.0 17.5.1r 17.05.01 ok
5  2C5A.0F1C.1EEC to 2C5A.0F1C.1EF6 2.0 17.5.1r 17.05.01 ok
6  2C5A.0F1C.1EF6 to 2C5A.0F1C.1F00 2.0 17.5.1r 17.05.01 ok
7  BC26.C7A4.D820 to BC26.C7A4.D84F 1.0 17.5.1r 17.05.01 ok
8  BC26.C772.E91C to BC26.C772.E94B 1.0 17.5.1r 17.05.01 ok
9  707D.B9C8.B5F8 to 707D.B9C8.B627 2.1 17.5.1r 17.05.01 ok
10 70EA.1ADB.7E74 to 70EA.1ADB.7EA3 3.0 17.5.1r 17.05.01 ok

```

Mod	Redundancy	Role	Operating Mode	Configured Mode	Redundancy Status
5	Active		sso	sso	Active
6	Standby		sso	sso	Standby Hot

Chassis MAC address range: 44 addresses from 2c5a.0f1c.1ec0 to 2c5a.0f1c.1eeb

Checking Interface Status

You can view summary or detailed information on the switch ports using the **show interface status** command. To see summary information on all ports on the switch, enter the **show interface status** command with no arguments. Specify a particular module number to see information on the ports on that module only. Enter both the module number and the port number to see detailed information about the specified port.

To apply configuration commands to a particular port, you must specify the appropriate logical module.

This example shows how to display the status of all interfaces on a Catalyst 9400 series switch, including transceivers:

```
Switch# show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi1/0/1		connected	1	a-full	a-1000	10/100/1000BaseTX
Gi1/0/2		connected	1	a-full	a-1000	10/100/1000BaseTX
Gi1/0/3		connected	1	a-full	a-1000	10/100/1000BaseTX
Gi1/0/4		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/5		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/6		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/7		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/8		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/9		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/10		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/11		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/12		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/13		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/14		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/15		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/16		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/17		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/18		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/19		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/20		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/21		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/22		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/23		notconnect	1	auto	auto	10/100/1000BaseTX
Gi1/0/24		notconnect	1	auto	auto	10/100/1000BaseTX

This example shows how to display the status of interfaces in error-disabled state:

```
Switch# show interfaces status err-disabled
Port Name Status Reason
```



```

Fa9/4 err-disabled link-flap
informational error message when the timer expires on a cause
-----
5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on Fa9/4
Switch#

```

Displaying MAC Addresses

In addition to displaying the MAC address range for a module using the **show module** command, you can display the MAC address table information of a specific MAC address or a specific interface in the switch using the **show mac address-table address** and **show mac address-table interface** commands

This example shows how to display MAC address table information for all MAC addresses:

```

Switch# show mac address-table
          Mac Address Table
-----
Vlan      Mac Address      Type      Ports
-----
All       0100.0ccc.cccc   STATIC    CPU
All       0100.0ccc.cccd   STATIC    CPU
All       0180.c200.0000   STATIC    CPU
All       0180.c200.0001   STATIC    CPU
All       0180.c200.0002   STATIC    CPU
All       0180.c200.0003   STATIC    CPU
All       0180.c200.0004   STATIC    CPU
All       0180.c200.0005   STATIC    CPU
All       0180.c200.0006   STATIC    CPU
All       0180.c200.0007   STATIC    CPU
All       0180.c200.0008   STATIC    CPU
All       0180.c200.0009   STATIC    CPU
All       0180.c200.000a   STATIC    CPU
All       0180.c200.000b   STATIC    CPU
All       0180.c200.000c   STATIC    CPU
All       0180.c200.000d   STATIC    CPU
All       0180.c200.000e   STATIC    CPU
All       0180.c200.000f   STATIC    CPU
All       0180.c200.0010   STATIC    CPU
All       0180.c200.0021   STATIC    CPU
All       ffff.ffff.ffff   STATIC    CPU
    1     188b.45eb.cc01   DYNAMIC   Gi1/0/1
Total Mac Addresses for this criterion: 22
Switch#

```

This example shows how to display MAC address table information for a specific interface:

```

Switch# show mac address-table interface Gi1/0/1
          Mac Address Table
-----
Vlan      Mac Address      Type      Ports
-----
    1     188b.45eb.cc01   DYNAMIC   Gi1/0/1
Total Mac Addresses for this criterion: 1
Switch#

```

Checking Cable Status Using Time Domain Reflectometer

The Time Domain Reflectometer (TDR) feature allows you to determine if cable is OPEN or SHORT when it is at fault.

With TDR, you can check the status of copper cables on the 48-port 10/100/1000 BASE-T modules for the Catalyst 9400 series switch. TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. All or part of the signal can be reflected back either by cable defects or by the end of the cable.

**Note**

Four pairs of standard category 5 cable exist. Each pair can assume one of the following states: open (not connected), broken, shorted, or terminated. The TDR test detects all four states and displays the first three as “Fault” conditions, and displays the fourth as “Terminated.” Although the CLI output is shown, the cable length is displayed only if the state is “Faulty.”

TDR feature is supported on the following modules:

- C9400-LC-48U
- C9400-LC-48T

TDR detects a cable fault by sending a signal along its wires and depending on the reflected signal it can determine roughly where a cable fault could be. The variations on how TDR signal is reflected back determine the results on TDR. On cat4k products, we only support cable fault types: OPEN or SHORT. We do display Terminated status in case cable is proper terminated and this is done for illustrative purpose.

Running the TDR Test

To start the TDR test, perform this task:

Procedure

	Command or Action	Purpose
Step 1	test cable-diagnostics tdr {interface { interface-number }}	Starts the TDR test.
Step 2	show cable-diagnostics tdr {interface interface-number}	Displays the TDR test counter information.

TDR Guidelines

The following guidelines apply to the use of TDR:

- Do not change the port configuration while the TDR test is running.
- If you connect a port undergoing a TDR test to an Auto-MDIX enabled port, the TDR result might be invalid. In those instances, the port on the device should be administratively down before the start of the TDR test.

- If you connect a port undergoing a TDR test to a 100BASE-T port such as that on the device, the unused pairs (4-5 and 7-8) is reported as faulty because the remote end does not terminate these pairs.
- Due to cable characteristics, you should run the TDR test multiple times to get accurate results.
- Do not change port status (for example, remove the cable at the near or far end) because the results might be inaccurate.
- TDR works best if the test cable is disconnected from the remote port. Otherwise, it might be difficult for you to interpret results correctly.
- TDR operates across four wires. Depending on the cable conditions, the status might show one pair is OPEN or SHORT while all other wire pairs display as faulty. This operation is acceptable because you should declare a cable faulty provided one pair of wires is either OPEN or SHORT.
- TDR intent is to determine how poorly a cable is functioning rather than to locate a faulty cable.
- When TDR locates a faulty cable, you should still use an offline cable diagnosis tool to better diagnose the problem.
- TDR results might differ between runs on different Catalyst 9400 modules because of the resolution difference of TDR implementations. When this occurs, you should refer to offline cable diagnosis tool.

Using Telnet

You can access the switch command-line interface (CLI) using Telnet. In addition, Telnet allows you to access other devices in the network. You can have up to eight simultaneous Telnet sessions.

Before you can open a Telnet session to the switch, you must first set the IP address (and in some cases the default gateway) for the switch. For information about setting the IP address and default gateway, see the section on Configuring the Switch for the First Time



Note To establish a Telnet connection to a host by using the hostname, configure and enable DNS.

To establish a Telnet connection to another device on the network from the switch, enter this command:

```
Switch# telnet host [port]
```

This example shows how to establish a Telnet connection from the switch to the remote host named labsparc:

```
Switch# telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.
UNIX(r) System V Release 4.0 (labsparc)
login:
```

Changing the Logout Timer

The logout timer automatically disconnects a user from the switch when the user is idle for longer than the specified time. To set the logout timer, enter this command:

```
Switch(config-line)# exec-timeout minutes seconds
```

This command changes the logout timer value (a timeout value of 0 prevents idle sessions from being disconnected automatically).

Use the **no** keyword to return to the default value.

To set the logout for 10 minutes and 10 seconds, enter the following command:

```
Switch(config)# line console 0
Switch(config-line)# exec-timeout 10 10
```

To set no logout timer for console session:

```
Switch(config)# line console 0
Switch(config-line)# exec-timeout 0 0
```

Monitoring User Sessions

You can display the currently active user sessions on the switch using the **show users** command. The command output lists all active console port and Telnet sessions on the switch.

To display the active user sessions on the switch, enter this command:

```
Switch# show users [all]
```

To disconnect an active user session on the switch, enter the following command:

```
Switch# disconnect { console | ip_address }
```

Example

This example shows the output of the show users command when local authentication is enabled for console and Telnet sessions (the asterisk [*] indicates the current session)

```
Switch# show users
Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00
Interface User Mode Idle Peer Address

Switch# show users all
Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00
1 vty 0 00:00:00
2 vty 1 00:00:00
3 vty 2 00:00:00
4 vty 3 00:00:00
5 vty 4 00:00:00
Interface User Mode Idle Peer Address
Switch#
```

This example shows how to disconnect an active console port session and an active Telnet session:

```
Switch> disconnect console
Console session disconnected.
Console> (enable) disconnect tim-nt.bigcorp.com
Telnet session from tim-nt.bigcorp.com disconnected. (1)
Switch# show users
Session User Location
-----
telnet jake jake-mac.bigcorp.com
* telnet suzy suzy-pc.bigcorp.com
Switch#
```

Using Ping

These sections describe how to use IP ping:

Understanding How Ping Works

The ping command allows you to verify connectivity to remote hosts. If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or configure a router to route between those subnets.

The ping command is configurable from normal executive and privileged EXEC mode. Ping returns one of the following responses:

- Normal response—The normal response (hostname is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a No Answer message is returned.
- Unknown host—If the host does not exist, an Unknown Host message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a Destination Unreachable message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a Network or Host Unreachable message is returned.

To stop a ping in progress, press Ctrl-C.

Running Ping

To ping another device on the network from the switch, enter this command in normal executive and privileged EXEC mode:

```
Switch# ping host
```

Checks connectivity to a remote host.

This example shows how to ping a remote host from normal executive mode:

```
Switch# ping labsparc
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#

Switch# ping 72.16.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 72.16.10.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

This example shows how to use a ping command in privileged EXEC mode to specify the number of packets, the packet size, and the timeout period:

```
Switch# ping
Protocol [ip]: ip
Target IP address: 1.1.1.1
Repeat count [5]: 10
Datagram size [100]: 100
Timeout in seconds [2]: 10
Extended commands [n]: n
Sweep range of sizes [n]: n
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 1.1.1.1, timeout is 10 seconds:
!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms
Switch#
```

Using IP Traceroute

Understanding How IP Traceroute Works

IP traceroute allows you to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Layer 2 switches can participate as the source or destination of the trace command but does not appear as a hop in the trace command output.

The trace command uses the time to live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an Internet Control Message Protocol (ICMP) Time-Exceeded message to the sender. Traceroute determines the address of the first hop by examining the source address field of the ICMP Time-Exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the Time-Exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host or until the maximum TTL is reached.

To determine when a datagram reaches its destination, traceroute sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP Port Unreachable error message to the source. The Port Unreachable error message indicates to traceroute that the destination has been reached.

Running IP Traceroute

To trace the path that packets take through the network, enter this command in EXEC or privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	traceroute [<i>protocol</i>] [<i>destination</i>]	Runs IP traceroute to trace the path that packets take through the network.

Example

This example shows how to use the traceroute command to display the route a packet takes through the network to reach its destination:

```
Switch# traceroute ip ABA.NYC.mil
Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
 1 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
 2 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
 3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
 4 BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
 5 SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
 6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
 7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
Switch#
```

Using Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. It determines the path by using the MAC address tables of the switches in the path. When the switch detects a device in the path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

If you want the switch to trace the path from a host on a source device to a host on a destination device, the switch can identify only the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Layer 2 Traceroute Usage Guidelines

These are the Layer 2 traceroute usage guidelines:

- CDP must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP.
If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.
- All switches in the physical path must have IP connectivity. When a switch is reachable from another switch, you can test connectivity by using the ping command in privileged EXEC mode.
- The maximum number of hops identified in the path is ten.
- You can enter the traceroute mac or the traceroute mac ip command in privileged EXEC mode on a switch that is not in the physical path from the source device to the destination device. All switches in the path must be reachable from this switch.

- The `traceroute mac` command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.
- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.
- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.
- The `traceroute mac ip` command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP address with the corresponding MAC address and the VLAN ID.
 - If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
 - If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.
- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.
- This feature is not supported in Token Ring VLANs.

Running Layer 2 Traceroute

To display the physical path that a packet takes from a source device to a destination device, enter either one of these commands:

```
Switch# traceroute mac source-mac-address destination-mac-address
```

OR

```
Switch# traceroute mac ip source-ip destination-ip
```

The following examples show how to use the `traceroute mac` and `traceroute mac ip` commands to display the physical path a packet takes through the network to reach its destination:

```
Switch# traceroute mac cc16.7eaa.7203 188b.45eb.cc64
Source cc16.7eaa.7203 found on Switch
1 Switch (1.1.1.1) : V11 => Gi1/0/1
Destination 188b.45eb.cc64 found on Switch
Layer 2 trace completed.
Switch#

Switch# traceroute mac ip 1.1.1.1 1.1.1.2 detail
Translating IP to mac .....
1.1.1.1 => cc16.7eaa.7203
1.1.1.2 => 188b.45eb.cc64

Source cc16.7eaa.7203 found on Switch[C9410R] (1.1.1.1)
1 Switch / C9410R / 1.1.1.1 :Gi1/0/1 [auto, auto]
Destination 188b.45eb.cc64 found on Switch[C9410R] (1.1.1.1)
```



```
Layer 2 trace completed.  
Switch#
```

Configuring ICMP

Internet Control Message Protocol (ICMP) provides many services that control and manage IP connections. ICMP messages are sent by routers or access servers to hosts or other routers when a problem is discovered with the Internet header. For detailed information on ICMP, refer RFC 792.

Enabling ICMP Protocol Unreachable Messages

If the Cisco IOS software receives a nonbroadcast packet that uses an unknown protocol, it sends an ICMP Protocol Unreachable message back to the source.

Similarly, if the software receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address, it sends an ICMP Host Unreachable message to the source. This feature is enabled by default.

To enable the generation of ICMP Protocol Unreachable and Host Unreachable messages, enter the following command in interface configuration mode:

```
Switch (config-if) # [no] ip unreachable
```

Use the **no** keyword to disable the ICMP destination unreachable messages.



Note If you enter the **no ip unreachable** command, you will break the path MTU discovery functionality. Routers in the middle of the network might be forced to fragment packets.

To limit the rate that Internet Control Message Protocol (ICMP) destination unreachable messages are generated, enter the following command:

```
Switch (config) # [no] ip icmp rate-limit unreachable [df] milliseconds
```

Use the **no** keyword to remove the rate limit and reduce the CPU usage.

Enabling ICMP Mask Reply Messages

Occasionally, network devices must know the subnet mask for a particular subnetwork in the internetwork. To obtain this information, devices can send ICMP Mask Request messages. These messages are responded to by ICMP Mask Reply messages from devices that have the requested information. The Cisco IOS software can respond to ICMP Mask Request messages if the ICMP Mask Reply function is enabled.

To have the Cisco IOS software respond to ICMP mask requests by sending ICMP Mask Reply messages, enter the following command:

```
Switch (config-if) # [no] ip mask-reply
```

Use the **no** keyword to disable this functionality.

Feature History for Checking Port Status and Connectivity

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.6.1	Port Status and Connectivity Check	This feature includes the steps to check the status of modules, and interfaces; and also how to verify connectivity between devices within the network.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 5

Configuring LLDP, LLDP-MED, and Wired Location Service

- [Restrictions for LLDP, on page 51](#)
- [Information About LLDP, LLDP-MED, and Wired Location Service, on page 51](#)
- [How to Configure LLDP, LLDP-MED, and Wired Location Service, on page 55](#)
- [Configuration Examples for LLDP, LLDP-MED, and Wired Location Service, on page 65](#)
- [Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service, on page 65](#)
- [Additional References for LLDP, LLDP-MED, and Wired Location Service, on page 66](#)
- [Feature History for LLDP, LLDP-MED, and Wired Location Service, on page 67](#)

Restrictions for LLDP

- If the interface is configured as a tunnel port, LLDP is automatically disabled.
- If you first configure a network-policy profile on an interface, you cannot apply the **switchport voice vlan** command on the interface. If the **switchport voice vlan *vlan-id*** is already configured on an interface, you can apply a network-policy profile on the interface. This way the interface has the voice or voice-signaling VLAN network-policy profile applied on the interface.
- You cannot configure static secure MAC addresses on an interface that has a network-policy profile.
- When Cisco Discovery Protocol and LLDP are both in use within the same switch, it is necessary to disable LLDP on interfaces where Cisco Discovery Protocol is in use for power negotiation. LLDP can be disabled at interface level with the commands **no lldp tlv-select power-management** or **no lldp transmit / no lldp receive**.

Information About LLDP, LLDP-MED, and Wired Location Service

LLDP

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, switches, and controllers). CDP allows

network management applications to automatically discover and learn about other Cisco devices connected to the network.

To support non-Cisco devices and to allow for interoperability between other devices, the device supports the IEEE 802.1AB Link Layer Discovery Protocol (LLDP). LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP Supported TLVs

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors. This protocol can advertise details such as configuration information, device capabilities, and device identity.

The switch supports these basic management TLVs. These are mandatory LLDP TLVs.

- Port description TLV
- System name TLV
- System description TLV
- System capabilities TLV
- Management address TLV

These organizationally specific LLDP TLVs are also advertised to support LLDP-MED.

- Port VLAN ID TLV (IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV (IEEE 802.3 organizationally specific TLVs)

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management and location information. By default, all LLDP-MED TLVs are enabled.

LLDP-MED Supported TLVs

LLDP-MED supports these TLVs:

- LLDP-MED capabilities TLV

Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and has enabled.

- Network policy TLV

Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. For example, the switch can notify a phone of the VLAN number that it should use. The phone can connect to any device, obtain its VLAN number, and then start communicating with the call control.

By defining a network-policy profile TLV, you can create a profile for voice and voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode. These profile attributes are then maintained centrally on the switch and propagated to the phone.

- Power management TLV

Enables advanced power management between LLDP-MED endpoint and network connectivity devices. Allows devices and phones to convey power information, such as how the device is powered, power priority, and how much power the device needs.

LLDP-MED also supports an extended power TLV to advertise fine-grained power requirements, end-point power priority, and end-point and network connectivity-device power status. LLDP is enabled and power is applied to a port, the power TLV determines the actual power requirement of the endpoint device so that the system power budget can be adjusted accordingly. The device processes the requests and either grants or denies power based on the current power budget. If the request is granted, the switch updates the power budget. If the request is denied, the device turns off power to the port, generates a syslog message, and updates the power budget. If LLDP-MED is disabled or if the endpoint does not support the LLDP-MED power TLV, the initial allocation value is used throughout the duration of the connection.

You can change power settings by entering the **power inline** {**auto** [**max** *max-wattage*] | **never** | **static** [**max** *max-wattage*] | **consumption** <**4000-60000**> **milliwatts**} interface configuration command. By default the PoE interface is in **auto** mode; If no value is specified, the maximum is allowed (60 W).

- Inventory management TLV

Allows an endpoint to send detailed inventory information about itself to the device, including information hardware revision, firmware version, software version, serial number, manufacturer name, model name, and asset ID TLV.

- Location TLV

Provides location information from the device to the endpoint device. The location TLV can send this information:

- Civic location information

Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.

- ELIN location information

Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

- Geographic location information

Provides the geographical details of a switch location such as latitude, longitude, and altitude of a switch.

- custom location

Provides customized name and value of a switch location.

Wired Location Service

The device uses the location service feature to send location and attachment tracking information for its connected devices to a Cisco Mobility Services Engine (MSE). The tracked device can be a wireless endpoint, a wired endpoint, or a wired device or controller. The device notifies the MSE of device link up and link down events through the Network Mobility Services Protocol (NMSP) location and attachment notifications.

The MSE starts the NMSP connection to the device, which opens a server port. When the MSE connects to the device there are a set of message exchanges to establish version compatibility and service exchange information followed by location information synchronization. After connection, the device periodically sends location and attachment notifications to the MSE. Any link up or link down events detected during an interval are aggregated and sent at the end of the interval.

When the device determines the presence or absence of a device on a link-up or link-down event, it obtains the client-specific information such as the MAC address, IP address, and username. If the client is LLDP-MED- or CDP-capable, the device obtains the serial number and UDI through the LLDP-MED location TLV or CDP.

Depending on the device capabilities, the device obtains this client information at link up:

- Slot and port specified in port connection
- MAC address specified in the client MAC address
- IP address specified in port connection
- 802.1X username if applicable
- Device category is specified as a *wired station*
- State is specified as *new*
- Serial number, UDI
- Model number
- Time in seconds since the device detected the association

Depending on the device capabilities, the device obtains this client information at link down:

- Slot and port that was disconnected
- MAC address
- IP address
- 802.1X username if applicable
- Device category is specified as a *wired station*
- State is specified as *delete*
- Serial number, UDI
- Time in seconds since the device detected the disassociation

When the device shuts down, it sends an attachment notification with the state *delete* and the IP address before closing the NMSP connection to the MSE. The MSE interprets this notification as disassociation for all the wired clients associated with the device.

If you change a location address on the device, the device sends an NMSP location notification message that identifies the affected ports and the changed address information.

Default LLDP Configuration

Table 6: Default LLDP Configuration

Feature	Default Setting
LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	2 seconds
LLDP tlv-select	Disabled to send and receive all TLVs
LLDP interface state	Disabled
LLDP receive	Disabled
LLDP transmit	Disabled
LLDP med-tlv-select	Disabled to send all LLDP-MED TLVs. When LLDP is globally enabled, LLDP-MED-TLV is also enabled.

How to Configure LLDP, LLDP-MED, and Wired Location Service

Enabling LLDP

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	lldp run Example: <pre>Device (config)# lldp run</pre>	Enables LLDP globally on the device.
Step 4	interface <i>interface-id</i> Example:	Specifies the interface on which you are enabling LLDP, and enter interface configuration mode.
Step 5	lldp transmit Example: <pre>Device (config-if)# lldp transmit</pre>	Enables the interface to send LLDP packets.
Step 6	lldp receive Example: <pre>Device (config-if)# lldp receive</pre>	Enables the interface to receive LLDP packets.
Step 7	end Example: <pre>Device (config-if)# end</pre>	Returns to privileged EXEC mode.
Step 8	show lldp Example: <pre>Device# show lldp</pre>	Verifies the configuration.
Step 9	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring LLDP Characteristics

You can configure the frequency of LLDP updates, the amount of time to hold the information before discarding it, and the initialization delay time. You can also select the LLDP and LLDP-MED TLVs to send and receive.



Note Steps 3 through 6 are optional and can be performed in any order.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	lldp holdtime <i>seconds</i> Example: <pre>Device(config)# lldp holdtime 120</pre>	(Optional) Specifies the amount of time a receiving device should hold the information from your device before discarding it. The range is 0 to 65535 seconds; the default is 120 seconds.
Step 4	lldp reinit <i>delay</i> Example: <pre>Device(config)# lldp reinit 2</pre>	(Optional) Specifies the delay time in seconds for LLDP to initialize on an interface. The range is 2 to 5 seconds; the default is 2 seconds.
Step 5	lldp timer <i>rate</i> Example: <pre>Device(config)# lldp timer 30</pre>	(Optional) Sets the sending frequency of LLDP updates in seconds. The range is 5 to 65534 seconds; the default is 30 seconds.
Step 6	lldp tlv-select Example: <pre>Device(config)# tlv-select</pre>	(Optional) Specifies the LLDP TLVs to send or receive.
Step 7	interface <i>interface-id</i> Example:	Specifies the interface on which you are enabling LLDP, and enter interface configuration mode.
Step 8	lldp med-tlv-select Example:	(Optional) Specifies the LLDP-MED TLVs to send or receive.

	Command or Action	Purpose
	Device (config-if)# lldp med-tlv-select inventory management	
Step 9	end Example: Device (config-if)# end	Returns to privileged EXEC mode.
Step 10	show lldp Example: Device# show lldp	Verifies the configuration.
Step 11	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring LLDP-MED TLVs

By default, the device only sends LLDP packets until it receives LLDP-MED packets from the end device. It then sends LLDP packets with MED TLVs, as well. When the LLDP-MED entry has been aged out, it again only sends LLDP packets.

By using the **lldp** interface configuration command, you can configure the interface not to send the TLVs listed in the following table.

Table 7: LLDP-MED TLVs

LLDP-MED TLV	Description
inventory-management	LLDP-MED inventory management TLV
location	LLDP-MED location TLV
network-policy	LLDP-MED network policy TLV
power-management	LLDP-MED power management TLV

Follow these steps to enable a TLV on an interface:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example:	Specifies the interface on which you are enabling LLDP, and enter interface configuration mode.
Step 4	lldp med-tlv-select Example: <pre>Device(config-if)# lldp med-tlv-select inventory management</pre>	Specifies the TLV to enable.
Step 5	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring Network-Policy TLV

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	network-policy profile <i>profile number</i> Example: <pre>Device(config)# network-policy profile 1</pre>	Specifies the network-policy profile number, and enter network-policy configuration mode. The range is 1 to 4294967295.
Step 4	{voice voice-signaling} vlan [vlan-id {cos cvalue dscp dvalue}] [[dot1p {cos cvalue dscp dvalue}] none untagged] Example: <pre>Device(config-network-policy)# voice vlan 100 cos 4</pre>	<p>Configures the policy attributes:</p> <ul style="list-style-type: none"> • voice—Specifies the voice application type. • voice-signaling—Specifies the voice-signaling application type. • vlan—Specifies the native VLAN for voice traffic. • vlan-id—(Optional) Specifies the VLAN for voice traffic. The range is 1 to 4094. • cos cvalue—(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5. • dscp dvalue—(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46. • dot1p—(Optional) Configures the telephone to use IEEE 802.1p priority tagging and use VLAN 0 (the native VLAN). • none—(Optional) Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad. • untagged—(Optional) Configures the telephone to send untagged voice traffic. This is the default for the telephone.

	Command or Action	Purpose
Step 5	exit Example: <pre>Device(config)# exit</pre>	Returns to global configuration mode.
Step 6	interface <i>interface-id</i> Example:	Specifies the interface on which you are configuring a network-policy profile, and enter interface configuration mode.
Step 7	network-policy <i>profile number</i> Example: <pre>Device(config-if)# network-policy 1</pre>	Specifies the network-policy profile number.
Step 8	lldp med-tlv-select network-policy Example: <pre>Device(config-if)# lldp med-tlv-select network-policy</pre>	Specifies the network-policy TLV.
Step 9	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 10	show network-policy profile Example: <pre>Device# show network-policy profile</pre>	Verifies the configuration.
Step 11	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring Location TLV and Wired Location Service

Beginning in privileged EXEC mode, follow these steps to configure location information for an endpoint and to apply it to an interface.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 2	location {admin-tag <i>string</i> civic-location identifier {<i>id</i> <i>host</i>} elin-location <i>string</i> identifier <i>id</i> custom-location identifier {<i>id</i> <i>host</i>} geo-location identifier {<i>id</i> <i>host</i>}} Example: <pre>Device(config)# location civic-location identifier 1 Device(config-civic)# number 3550 Device(config-civic)# primary-road-name "Cisco Way" Device(config-civic)# city "San Jose" Device(config-civic)# state CA Device(config-civic)# building 19 Device(config-civic)# room C6 Device(config-civic)# county "Santa Clara" Device(config-civic)# country US</pre>	Specifies the location information for an endpoint. <ul style="list-style-type: none"> • admin-tag—Specifies an administrative tag or site information. • civic-location—Specifies civic location information. • elin-location—Specifies emergency location information (ELIN). • custom-location—Specifies custom location information. • geo-location—Specifies geo-spatial location information. • identifier <i>id</i>—Specifies the ID for the civic, ELIN, custom, or geo location. • host—Specifies the host civic, custom, or geo location. • <i>string</i>—Specifies the site or location information in alphanumeric format.
Step 3	exit Example: <pre>Device(config-civic)# exit</pre>	Returns to global configuration mode.
Step 4	interface <i>interface-id</i> Example:	Specifies the interface on which you are configuring the location information, and enter interface configuration mode.
Step 5	location {additional-location-information <i>word</i> civic-location-id {<i>id</i> <i>host</i>} elin-location-id <i>id</i> custom-location-id {<i>id</i> <i>host</i>} geo-location-id {<i>id</i> <i>host</i>}} Example: <pre>Device(config-if)# location</pre>	Enters location information for an interface: <ul style="list-style-type: none"> • additional-location-information—Specifies additional information for a location or place. • civic-location-id—Specifies global civic location information for an interface.

	Command or Action	Purpose
	<code>elin-location-id 1</code>	<ul style="list-style-type: none"> • elin-location-id—Specifies emergency location information for an interface. • custom-location-id—Specifies custom location information for an interface. • geo-location-id—Specifies geo-spatial location information for an interface. • host—Specifies the host location identifier. • word—Specifies a word or phrase with additional location information. • id—Specifies the ID for the civic, ELIN, custom, or geo location. The ID range is 1 to 4095.
Step 6	end Example: <code>Device(config-if)# end</code>	Returns to privileged EXEC mode.
Step 7	Use one of the following: <ul style="list-style-type: none"> • show location admin-tag <i>string</i> • show location civic-location identifier <i>id</i> • show location elin-location identifier <i>id</i> Example: <code>Device# show location admin-tag</code> or <code>Device# show location civic-location identifier</code> or <code>Device# show location elin-location identifier</code>	Verifies the configuration.
Step 8	copy running-config startup-config Example: <code>Device# copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Enabling Wired Location Service on the Device

Before you begin

For wired location to function, you must first enter the **ip device tracking** global configuration command.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	nmosp notification interval {attachment location} interval-seconds Example: <pre>Device(config)# nmosp notification interval location 10</pre>	Specifies the NMSP notification interval. attachment —Specifies the attachment notification interval. location —Specifies the location notification interval. <i>interval-seconds</i> —Duration in seconds before the device sends the MSE the location or attachment updates. The range is 1 to 30; the default is 30.
Step 4	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show network-policy profile Example: <pre>Device# show network-policy profile</pre>	Verifies the configuration.
Step 6	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuration Examples for LLDP, LLDP-MED, and Wired Location Service

Configuring Network-Policy TLV: Examples

This example shows how to configure VLAN 100 for voice application with CoS and to enable the network-policy profile and network-policy TLV on an interface:

```
# configure terminal
(config)# network-policy 1
(config-network-policy)# voice vlan 100 cos 4
(config-network-policy)# exit
(config)# interface gigabitethernet1/0/1
(config-if)# network-policy profile 1
(config-if)# lldp med-tlv-select network-policy
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

```
config-network-policy)# voice vlan dot1p cos 4
config-network-policy)# voice vlan dot1p dscp 34
```

Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service

Commands for monitoring and maintaining LLDP, LLDP-MED, and wired location service.

Command	Description
clear lldp counters	Resets the traffic counters to zero.
clear lldp table	Deletes the LLDP neighbor information table.
clear nmstp statistics	Clears the NMSP statistic counters.
show lldp	Displays global information, such as frequency of transmissions, the holdtime for packets being sent, and the delay time before LLDP initializes on an interface.
show lldp entry <i>entry-name</i>	Displays information about a specific neighbor. You can enter an asterisk (*) to display all neighbors, or you can enter the neighbor name.

Command	Description
show lldp interface [<i>interface-id</i>]	Displays information about interfaces with LLDP enabled. You can limit the display to a specific interface.
show lldp neighbors [<i>interface-id</i>] [detail]	Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID. You can limit the display to neighbors of a specific interface or expand the display for more detailed information.
show lldp traffic	Displays LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.
show location admin-tag <i>string</i>	Displays the location information for the specified administrative tag or site.
show location civic-location identifier <i>id</i>	Displays the location information for a specific global civic location.
show location elin-location identifier <i>id</i>	Displays the location information for an emergency location
show network-policy profile	Displays the configured network-policy profiles.
show nmosp	Displays the NMSP information

Additional References for LLDP, LLDP-MED, and Wired Location Service

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for LLDP, LLDP-MED, and Wired Location Service

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.6.1	Link Layer Discovery Protocol (LLDP), LLDP-MED, Wired Location Service	<p>LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.</p> <p>LLDP-MED operates between endpoints and network devices.</p> <p>Wired Location Service lets you send tracking information of the connected devices to a Cisco Mobility Services Engine (MSE)</p>

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 6

Configuring System MTU

- [Restrictions for System MTU, on page 69](#)
- [Information About the MTU, on page 69](#)
- [How to Configure MTU , on page 70](#)
- [Configuration Examples for System MTU, on page 71](#)
- [Additional References for System MTU, on page 72](#)
- [Feature History for System MTU, on page 72](#)

Restrictions for System MTU

When configuring the system MTU values, follow these guidelines:

- The device does not support the MTU on a per-interface basis.
- If you enter the **system mtu bytes** command in global configuration mode, the command affects all the switched and routed ports on the switch.

Information About the MTU

The default maximum transmission unit (MTU) size for payload received in Ethernet frame and sent on all device interfaces is 1500 bytes.

System MTU Value Application

This table shows how the MTU values are applied.

Table 8: MTU Values

Configuration	system mtu command
Standalone switch	You can enter the system mtu command on a switch, but system MTU value does not take effect on the switch. It affects the Fast Ethernet ports. The range is from 1500 to 9198 bytes.

For more information about setting the MTU sizes, see the **system mtu** global configuration command in the command reference for this release.

How to Configure MTU

Configuring the System MTU

Follow these steps to change the MTU size for switched packets:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	system mtu bytes Example: Device(config)# system mtu 1900	(Optional) Changes the MTU size for all interfaces.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	Saves your entries in the configuration file.
Step 6	show system mtu Example: Device# show system mtu	Verifies your settings.

Configuring Protocol-Specific MTU

To override system MTU values on routed interfaces, configure protocol-specific MTU under each routed interface. To change the MTU size for routed ports, perform this procedure

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface interface Example: Device(config)# interface gigabitethernet0/0	Enters interface configuration mode.
Step 3	ip mtu bytes Example: Device(config-if)# ip mtu 68	Changes the IPv4 MTU size
Step 4	ipv6 mtu bytes Example: Device(config-if)# ipv6 mtu 1280	(Optional) Changes the IPv6 MTU size.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	Saves your entries in the configuration file.
Step 7	show system mtu Example: Device# show system mtu	Verifies your settings.

Configuration Examples for System MTU

Example: Configuring Protocol-Specific MTU

Example: Configuring the System MTU

```

Device# configure terminal
Device(config)# system mtu 1600
Device(config)# exit

```

Additional References for System MTU

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for System MTU

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.6.1	System MTU	System MTU defines the maximum transmission unit size for frames transmitted on all interfaces of a switch.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 7

Configuring COAP Proxy Server

- [Restrictions for the COAP Proxy Server, on page 73](#)
- [Information About the COAP Proxy Server, on page 73](#)
- [How to Configure the COAP Proxy Server, on page 74](#)
- [Configuration Examples for the COAP Proxy Server, on page 77](#)
- [Monitoring COAP Proxy Server, on page 81](#)
- [Feature Information for COAP, on page 82](#)

Restrictions for the COAP Proxy Server

The following restrictions apply to COAP proxy server:

- Switch cannot advertise itself as CoAP client using ipv6 broadcast (CSCuw26467).
- Support for Observe Not Implemented.
- Blockwise requests are not supported. We handle block-wise responses and can generate block-wise responses.
- DTLS Support is for the following modes only RawPublicKey and Certificate Based.
- Switch does not act as DTLS client. DTLS for endpoints only.
- Endpoints are expected to handle and respond with CBOR payloads.
- Client side requests are expected to be in JSON.
- Switch cannot advertise itself to other Resource Directories as IPv6, due to an IPv6 broadcast issue.

Information About the COAP Proxy Server

The COAP protocol is designed for use with constrained devices. COAP works in the same way on constrained devices as HTTP works on servers in accessing information.

The comparison of COAP and HTTP is shown below:

- In the case of a webserver: **HTTP** is the protocol; **TCP** is the transport; and **HTML** is the most common information format transported.

- In case of a constrained device: **COAP** is the protocol; **UDP** is the transport; and **JSON/link-format/CBOR** is the popular information format.

COAP provides a means to access and control device using a similar **GET/POST** metaphor and restful API as in HTTP.

How to Configure the COAP Proxy Server

To configure the COAP proxy server, you can configure the COAP Proxy and COAP Endpoints in the Configuration mode.

The commands are: **coap [proxy | endpoints]**.

Configuring the COAP Proxy

To start or stop the COAP proxy on the switch, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	coap proxy Example: <pre>Device(config)# coap proxy</pre>	Enters the COAP proxy sub mode. Note To stop the coap proxy and delete all configurations under coap proxy, use the no coap proxy command.
Step 4	security [none [[ipv4 ipv6] {ip-address ip-mask/prefix} list {ipv4-list name / ipv6-list-name}]] dtls [id-trustpoint {identity-trustpoint label}]] [verification-trustpoint {verification-trustpoint} [ipv4 ipv6 {ip-address ip-mask/prefix}]] list {ipv4-list name ipv6-list-name}]] Example: <pre>Device(config-coap-proxy)# security none</pre>	Takes the encryption type as argument. The two security modes supported are none and dtls <ul style="list-style-type: none"> • none - Indicates no security on that port. With security none, a maximum of 5 ipv4 and 5 ipv6 addresses can be associated. • dtls - The DTLS security takes RSA trustpoint and Verification trustpoint which are optional. Without Verification

	Command or Action	Purpose
	<code>ipv4 1.1.0.0 255.255.0.0</code>	trustpoint it does the normal Public Key Exchange. With security dtls , a maximum of 5 ipv4 and 5 ipv6 addresses can be associated. Note To delete all security configurations under coap proxy, use the no security command.
Step 5	max-endpoints { <i>number</i> } Example: Device (config-coap-proxy) # max-endpoints 10	(Optional) Specifies the maximum number of endpoints that can be learnt on the switch. The default value is 10. The range is 1 to 500. Note To delete all max-endpoints configured under coap proxy, use the no max-endpoints command.
Step 6	port-unsecure { <i>port-num</i> } Example: Device (config-coap-proxy) # port-unsecure 5683	(Optional) Configures a port other than the default 5683. The range is 1 to 65000. Note To delete all port configurations under coap proxy, use the no port-unsecure command.
Step 7	port-dtls { <i>port-num</i> } Example: Device (config-coap-proxy) # port-dtls 5864	(Optional) Configures a port other than the default 5684. Note To delete all dtls port configurations under coap proxy, use the no port-dtls command.
Step 8	resource-directory [ipv4 ipv6] { <i>ip-address</i> }] Example: Device (config-coap-proxy) # resource-directory ipv4 192.168.1.1	Configures a unicast upstream resource directory server to which the switch can act as a COAP client. With resource-directory , a maximum of 5 of ipv4 and 5 ipv6, ip addresses can be configured. Note To delete all resource directory configurations under coap proxy, use the no resource-directory command.
Step 9	list [ipv4 ipv6] { <i>list-name</i> } Example: Device (config-coap-proxy) # list ipv4 trial_list	(Optional) Restricts the IP address range where the lights and their resources can be learnt. Creates a named list of ip address/masks, to be used in the security [none dtls] command options above.

	Command or Action	Purpose
		<p>With list, a maximum of 5 ip-lists can be configured, irrespective of ipv4 or ipv6. We can configure a max of 5 ip addresses per ip-list.</p> <p>Note To delete any ip list on the COAP proxy server, use the no list [ipv4 ipv6] {list-name} command.</p>
Step 10	start Example: Device(config-coap-proxy)# start	Starts the COAP proxy on this switch.
Step 11	stop Example: Device(config-coap-proxy)# stop	Stops the COAP proxy on this switch.
Step 12	exit Example: Device(config-coap-proxy)# exit	Exits the COAP proxy sub mode.
Step 13	end Example: Device(config)# end	Returns to privileged EXEC mode.

Configuring COAP Endpoints

To configure the COAP Proxy to support multiple IPv4/IPv6 static-endpoints, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	coap endpoint [ipv4 ipv6] {ip-address} Example: <pre>Device(config)#coap endpoint ipv4 1.1.1.1 Device(config)#coap endpoint ipv6 2001::1</pre>	Configures the static endpoints on the switch. <ul style="list-style-type: none"> • ipv4 - Configures the IPv4 Static endpoints. • ipv6 - Configures the IPv6 Static endpoints. <p>Note To stop the coap proxy on any endpoint, use the no coap endpoint [ipv4 ipv6] {ip-address} command.</p>
Step 4	exit Example: <pre>Device(config-coap-endpoint)# exit</pre>	Exits the COAP endpoint sub mode.
Step 5	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.

Configuration Examples for the COAP Proxy Server

Examples: Configuring the COAP Proxy Server

This example shows how you can configure the port number 5683 to support a maximum of 10 endpoints.

```
Device#coap proxy security none ipv4 2.2.2.2 255.255.255.0 port 5683 max-endpoints 10
```

This example shows how to configure COAP proxy on *ipv4 1.1.0.0 255.255.0.0* with **no** security settings.

```
Device(config-coap-proxy)# security ?
dtls  dtls
none  no security
```

```
Device(config-coap-proxy)#security none ?
ipv4    IP address range on which to learn lights
ipv6    IPv6 address range on which to learn lights
```

```

list      IP address range on which to learn lights

Device(config-coap-proxy)#security none ipv4 ?
A.B.C.D  {/nn || A.B.C.D}  IP address range on which to learn lights

Device(config-coap-proxy)#security none ipv4 1.1.0.0 255.255.0.0

```

This example shows how to configure COAP proxy on *ipv4 1.1.0.0 255.255.0.0* with **dtls id trustpoint** security settings.

```

Device(config-coap-proxy)#security dtls ?
id-trustpoint DTLS RSA and X.509 Trustpoint Labels
ipv4 IP address range on which to learn lights
ipv6 IPv6 address range on which to learn lights
list IP address range on which to learn lights

Device(config-coap-proxy)#security dtls id-trustpoint ?
WORD      Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT ?
verification-trustpoint Certificate Verification Label
<cr>

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT

Device(config-coap-proxy)#security dtls ?
id-trustpoint DTLS RSA and X.509 Trustpoint Labels
ipv4 IP address range on which to learn lights
ipv6 IPv6 address range on which to learn lights
list IP address range on which to learn lights

Device(config-coap-proxy)# security dtls ipv4 1.1.0.0 255.255.0.0

```



Note For configuring **ipv4 / ipv6 / list**, the **id-trustpoint** and (optional) **verification-trustpoint**, should be pre-configured, else the system shows an error.

This example shows how to configure a Trustpoint. This is a pre-requisite for COAP **security dtls** with **id trustpoint** configurations.

```

ip domain-name myDomain
crypto key generate rsa general-keys exportable label MyLabel modulus 2048

Device(config)#crypto pki trustpoint MY_TRUSTPOINT
Device(ca-trustpoint)#rsakeypair MyLabel 2048
Device(ca-trustpoint)#enrollment selfsigned
Device(ca-trustpoint)#exit

Device(config)#crypto pki enroll MY_TRUSTPOINT
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

```

This example shows how to configure COAP proxy on *ipv4 1.1.0.0 255.255.0.0* with **dtls verification trustpoint** (DTLS with certificates or verification trustpoints)

```
Device(config-coap-proxy)#security dtls ?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights

Device(config-coap-proxy)#security dtls id-trustpoint ?
  WORD Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT ?
  verification-trustpoint Certificate Verification Label
  <cr>

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT verification-trustpoint
?
  WORD Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT verification-trustpoint
CA-TRUSTPOINT ?
  <cr>
```

This example shows how to configure Verification Trustpoint. This is a pre-requisite for COAP **security dtls** with **verification trustpoint** configurations.

```
Device(config)#crypto pki import CA-TRUSTPOINT pkcs12 flash:hostA.p12 password cisco123
% Importing pkcs12...
Source filename [hostA.p12]?
Reading file from flash:hostA.p12
CRYPTO_PKI: Imported PKCS12 file successfully.
```

This example shows how to create a list named trial-list, to be used in the security [none | dtls] command options.

```
Device(config-coap-proxy)#list ipv4 trial_list
Device(config-coap-proxy-iplist)#1.1.0.0 255.255.255.0
Device(config-coap-proxy-iplist)#2.2.0.0 255.255.255.0
Device(config-coap-proxy-iplist)#3.3.0.0 255.255.255.0
Device(config-coap-proxy-iplist)#exit
Device(config-coap-proxy)#security none list trial_list
```

This example shows all the negation commands available in the coap-proxy sub mode.

```
Device(config-coap-proxy)#no ?
  ip-list          Configure IP-List
  max-endpoints    maximum number of endpoints supported
  port-unsecure    Specify a port number to use
  port-dtls        Specify a dtls-port number to use
  resource-discovery Resource Discovery Server
  security         CoAP Security features
```

This example shows how you can configure multiple IPv4/IPv6 static-endpoints on the coap proxy.

```
Device(config)# coap endpoint ipv4 1.1.1.1
Device(config)# coap endpoint ipv4 2.1.1.1
Device(config)# coap endpoint ipv6 2001::1
```

This example shows how you can display the COAP protocol details.

```
Device#show coap version
CoAP version 1.0.0
RFC 7252
```

```
Device#show coap resources
Link format data =
</>
</1.1.1.6/cisco/context>
</1.1.1.6/cisco/actuator>
</1.1.1.6/cisco/sensor>
</1.1.1.6/cisco/lldp>
</1.1.1.5/cisco/context>
</1.1.1.5/cisco/actuator>
</1.1.1.5/cisco/sensor>
</1.1.1.5/cisco/lldp>
</cisco/flood>
</cisco/context>
</cisco/showtech>
</cisco/lldp>
```

```
Device#show coap globals
Coap System Timer Values :
  Discovery   : 120 sec
  Cache Exp   : 5 sec
  Keep Alive  : 120 sec
  Client DB   : 60 sec
  Query Queue : 500 ms
  Ack delay   : 500 ms
  Timeout     : 5 sec
```

```
Max Endpoints      : 10
Resource Disc Mode : POST
```

```
Device#show coap stats
Coap Stats :
Endpoints : 2
Requests : 20
Ext Queries : 0
```

```
Device#show coap endpoints
List of all endpoints :
```

```
Code : D - Discovered , N - New
#      Status   Age(s)  LastWKC(s)  IP
-----
1      D         10      94            1.1.1.6
```



```
2      D          6          34          1.1.1.5
```

```
Endpoints - Total : 2 Discovered : 2 New : 0
```

```
Device#show coap dtls-endpoints
```

```
#      Index State  String State      Value  Port IP
-----
1      3      SSLOK    3          48969  20.1.1.30
2      2      SSLOK    3          53430  20.1.1.31
3      4      SSLOK    3          54133  20.1.1.32
4      7      SSLOK    3          48236  20.1.1.33
```

This example shows all options available to debug the COAP protocol.

```
Device#debug coap ?
```

```
all          Debug CoAP all
database     Debug CoAP Database
errors       Debug CoAP errors
events       Debug CoAP events
packet       Debug CoAP packet
trace        Debug CoAP Trace
warnings     Debug CoAP warnings
```

Monitoring COAP Proxy Server

To display the COAP protocol details, use the commands in the following table:

Table 9: Commands to Display to COAP specific data

show coap version	Shows the IOS COAP version and the RFC information.
show coap resources	Shows the resources of the switch and those learnt by it.
show coap endpoints	Shows the endpoints which are discovered and learnt.
show coap globals	Shows the timer values and end point values.
show coap stats	Shows the message counts for endpoints, requests and external queries.
show coap dtls-endpoints	Shows the dtls endpoint status.

Table 10: Commands to Clear COAP Commands

clear coap database	Clears the COAP learnt on the switch, and the internal database of endpoint information.
----------------------------	--

To debug the COAP protocol, use the commands in the following table:

Table 11: Commands to Debug COAP protocol

debug coap database	Debugs the COAP database output.
debug coap errors	Debugs the COAP errors output.
debug coap events	Debugs the COAP events output.
debug coap packets	Debugs the COAP packets output.
debug coap trace	Debugs the COAP traces output.
debug coap warnings	Debugs the COAP warnings output.
debug coap all	Debugs all the COAP output.



Note

If you wish to disable the debugs, prepend the command with a "no" keyword.

Feature Information for COAP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12: Feature Information for COAP

Feature Name	Releases	Feature Information
COAP	Cisco IOS XE Everest 16.6.1	The COAP protocol is designed for use with constrained devices. COAP works in the same way on constrained devices as HTTP works on servers in accessing information.



CHAPTER 8

Configuring 2-event Classification

- [Restrictions for 2-event classification, on page 83](#)
- [Information about 2-event Classification, on page 83](#)
- [Configuring 2-event Classification, on page 83](#)
- [Example: Configuring 2-Event Classification, on page 84](#)
- [Feature Information for 2-event Classification, on page 84](#)

Restrictions for 2-event classification

The following restrictions apply to 2-event classification:

- Configuration of 2-event classification has to be done before physically connecting any endpoint. Alternatively do a manual shut/no-shut of the ports drawing power.
- Power to the ports will be interrupted in case of MCU firmware upgrade and ports will be back up immediately after the upgrade.

Information about 2-event Classification

When a class 4 device gets detected, IOS allocates 30W without any CDP or LLDP negotiation. This means that even before the link comes up the class 4 power device gets 30W.

Also, on the hardware level the PSE does a 2-event classification which allows a class 4 PD to detect PSE capability of providing 30W from hardware, register itself and it can move up to PoE+ level without waiting for any CDP/LLDP packet exchange.

Once 2-event is enabled on a port, you need to manually shut/un-shut the port or connect the PD again to start the IEEE detection again. Power budget allocation for a class-4 device will be 30W if 2-event classification is enabled on the port, else it will be 15.4W.

Configuring 2-event Classification

To configure the switch for a 2-event Classification, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet2/0/1	Specifies the physical port to be configured, and enters interface configuration mode.
Step 4	power inline port 2-event Example: Device(config-if)# power inline port 2-event	Configures 2-event classification on the switch.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Example: Configuring 2-Event Classification

This example shows how you can configure 2-event classification.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# power inline port 2-event
Device(config-if)# end
```

Feature Information for 2-event Classification

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 13: Feature Information for 2-event Classification

Feature Name	Releases	Feature Information
2-event classification	Cisco IOS XE Everest 16.6.1	When a class 4 device gets detected, IOS allocates 30W without any CDP or LLDP negotiation. This means that even before the link comes up the class 4 power device gets 30W.



CHAPTER 9

Configuring PoE

- [Information About PoE, on page 87](#)
- [How to Configure PoE and UPoE, on page 92](#)
- [Monitoring Power Status, on page 96](#)
- [Additional References for PoE, on page 97](#)
- [Feature History for Power over Ethernet, on page 97](#)

Information About PoE

PoE and PoE+ Ports

A PoE-capable switch port automatically supplies power to one of these connected devices if the device senses that there is no power on the circuit:

- A Cisco prestandard powered device (such as a Cisco IP Phone)
- An IEEE 802.3af-compliant powered device
- An IEEE 802.3at-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

Supported Protocols and Standards

The device uses the following protocols and standards to support PoE:

- CDP with power consumption—The powered device notifies the device of the amount of power it is consuming. The device does not reply to the power-consumption messages. The device can only supply power to or remove power from the PoE port.
- Cisco intelligent power management—The powered device and the device negotiate through power-negotiation CDP messages for an agreed-upon power-consumption level. The negotiation allows a Cisco powered device, that requires different power levels than its current allocation, to operate. The powered device first boots with its IEEE class power or 15.4W (pre-standard Cisco PD), then negotiates power to operate at appropriate power level. The device consumption changes to requested power mode only when it receives confirmation from the device.

High-power devices can operate in low-power mode on devices that do not support power-negotiation CDP.

Cisco intelligent power management is backward-compatible with CDP with power consumption; the device responds according to the CDP message that it receives. CDP is not supported on third-party powered devices; therefore, the device uses the IEEE classification to determine the power usage of the device.

- IEEE 802.3af—The major features of this standard are powered-device discovery, power administration, disconnect detection, and optional powered-device power classification. For more information, see the standard.
- IEEE 802.3at—The PoE+ standard increases the maximum power that can be drawn by a powered device from 15.4 W per port to 30 W per port.
- The Cisco UPOE feature provides the capability to source up to 60 W of power (2 x 30 W) over both signal and spare pairs of the RJ-45 Ethernet cable by using the Layer-2 power negotiation protocols such as CDP or LLDP. An LLDP and CDP request of 30 W and higher in presence of the 4-wire Cisco Proprietary spare-pair power TLV can provide power on the spare pair.

Related Topics

[Cisco Universal Power Over Ethernet](#), on page 91

Powered-Device Detection and Initial Power Allocation

The device detects a Cisco pre-standard or an IEEE-compliant powered device when the PoE-capable port is in the no-shutdown state, PoE is enabled (the default), and the connected device is not being powered by an AC adaptor.

After device detection, the device determines the device power requirements based on its type:

- The initial power allocation is the maximum amount of power that a powered device requires. The device initially allocates this amount of power when it detects and powers the powered device. As the device receives CDP messages from the powered device and as the powered device negotiates power levels with the device through CDP power-negotiation messages, the initial power allocation might be adjusted.
- The device classifies the detected IEEE device within a power consumption class. Based on the available power in the power budget, the device determines if a port can be powered. Following *IEEE Power Classifications* table lists these levels.

Table 14: IEEE Power Classifications

Class	Maximum Power Level Required from the Device
0 (class status unknown)	15.4 W
1	4 W
2	7 W
3	15.4 W

The device monitors and tracks requests for power and grants power only when it is available. The device tracks its power budget (the amount of power available on the device for PoE). The device performs power-accounting calculations when a port is granted or denied power to keep the power budget up to date.

After power is applied to the port, the device uses CDP to determine the *CDP-specific* power consumption requirement of the connected Cisco powered devices, which is the amount of power to allocate based on the CDP messages. The device adjusts the power budget accordingly. This does not apply to third-party PoE devices. The device processes a request and either grants or denies power. If the request is granted, the device updates the power budget. If the request is denied, the device ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. Powered devices can also negotiate with the device for more power.

With PoE+, powered devices use IEEE 802.3at and LLDP power with media dependent interface (MDI) type, length, and value descriptions (TLVs), Power-via-MDI TLVs, for negotiating power up to 30 W. Cisco pre-standard devices and Cisco IEEE powered devices can use CDP or the IEEE 802.3at power-via-MDI power negotiation mechanism to request power levels up to 30 W.



Note The initial allocation for Class 4 powered devices is 15.4 W. When a device starts up and uses CDP or LLDP to send a request for more than 15.4 W, it can be allocated up to the maximum of 30 W.



Note The CDP-specific power consumption requirement is referred to as the *actual* power consumption requirement in the software configuration guides and command references.

If the device detects a fault caused by an undervoltage, overvoltage, overtemperature, oscillator-fault, or short-circuit condition, it turns off power to the port, generates a syslog message, and updates the power budget and LEDs.

Power Management Modes

The device supports these PoE modes:

- **auto**—The device automatically detects if the connected device requires power. If the device discovers a powered device connected to the port and if the device has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the LEDs. For LED information, see the hardware installation guide.

If the device has enough power for all the powered devices, they all come up. If enough power is available for all powered devices connected to the device, power is turned on to all devices. If there is not enough available PoE, or if a device is disconnected and reconnected while other devices are waiting for power, it cannot be determined which devices are granted or are denied power.

If granting power would exceed the system power budget, the device denies power, ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. After power has been denied, the device periodically rechecks the power budget and continues to attempt to grant the request for power.

If a device being powered by the device is then connected to wall power, the device might continue to power the device. The device might continue to report that it is still powering the device whether the device is being powered by the device or receiving power from an AC power source.

If a powered device is removed, the device automatically detects the disconnect and removes power from the port. You can connect a nonpowered device without damaging it.

You can specify the maximum wattage that is allowed on the port. If the IEEE class maximum wattage of the powered device is greater than the configured maximum value, the device does not provide power to the port. If the device powers a powered device, but the powered device later requests through CDP

messages more than the configured maximum value, the device removes power to the port. The power that was allocated to the powered device is reclaimed into the global power budget. If you do not specify a wattage, the device delivers the maximum value. Use the **auto** setting on any PoE port. The auto mode is the default setting.

- **static**—The device pre-allocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port. The device allocates the port configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come, first-served model.

However, if the powered-device IEEE class is greater than the maximum wattage, the device does not supply power to it. If the device learns through CDP messages that the powered device is consuming more than the maximum wattage, the device shuts down the powered device.

If you do not specify a wattage, the device pre-allocates the maximum value. The device powers the port only if it discovers a powered device. Use the **static** setting on a high-priority interface.

- **never**—The device disables powered-device detection and never powers the PoE port even if an unpowered device is connected. Use this mode only when you want to make sure that power is never applied to a PoE-capable port, making the port a data-only port.

For most situations, the default configuration (auto mode) works well, providing plug-and-play operation. No further configuration is required. However, perform this task to configure a PoE port for a higher priority, to make it data only, or to specify a maximum wattage to disallow high-power powered devices on a port.

Power Monitoring and Power Policing

When policing of the real-time power consumption is enabled, the device takes action when a powered device consumes more power than the maximum amount allocated, also referred to as the *cutoff-power value*.

When PoE is enabled, the device senses the real-time power consumption of the powered device. The device monitors the real-time power consumption of the connected powered device; this is called *power monitoring* or *power sensing*. The device also polices the power usage with the *power policing* feature.

Power monitoring is backward-compatible with Cisco intelligent power management and CDP-based power consumption. It works with these features to ensure that the PoE port can supply power to the powered device.

The device senses the real-time power consumption of the connected device as follows:

1. The device monitors the real-time power consumption on individual ports.
2. The device records the power consumption, including peak power usage. The device reports the information through the CISCO-POWER-ETHERNET-EXT-MIB.
3. If power policing is enabled, the device polices power usage by comparing the real-time power consumption to the maximum power allocated to the device. The maximum power consumption is also referred to as the *cutoff power* on a PoE port.

If the device uses more than the maximum power allocation on the port, the device can either turn off power to the port, or the device can generate a syslog message and update the LEDs (the port LED is now blinking amber) while still providing power to the device based on the device configuration. By default, power-usage policing is disabled on all PoE ports.

If error recovery from the PoE error-disabled state is enabled, the device automatically takes the PoE port out of the error-disabled state after the specified amount of time.

If error recovery is disabled, you can manually re-enable the PoE port by using the **shutdown** and **no shutdown** interface configuration commands.

4. If policing is disabled, the powered device can receive a maximum power of 15.4W (the port default maximum limit is 15.4W). If the powered device consumes more than this limit, the port goes to faulty state.

Power Consumption Values

You can configure the initial power allocation and the maximum power allocation on a port. However, these values are only the configured values that determine when the device should turn on or turn off power on the PoE port. The maximum power allocation is not the same as the actual power consumption of the powered device. The actual cutoff power value that the device uses for power policing is not equal to the configured power value.

When power policing is enabled, the device polices the power usage *at the switch port*, which is greater than the power consumption of the device. When you manually set the maximum power allocation, you must consider the power loss over the cable from the switch port to the powered device. The cutoff power is the sum of the rated power consumption of the powered device and the worst-case power loss over the cable.

We recommend that you enable power policing when PoE is enabled on your device. For example, for a Class 1 device, if policing is disabled and you set the cutoff-power value by using the **power inline auto max 6300** interface configuration command, the configured maximum power allocation on the PoE port is 6.3 W (6300 mW). The device provides power to the connected devices on the port if the device needs up to 6.3 W. If the CDP-power negotiated value or the IEEE classification value exceeds the configured cutoff value, the device does not provide power to the connected device. After the device turns on power on the PoE port, the device does not police the real-time power consumption of the device, and the device can consume more power than the maximum allocated amount, which could adversely affect the device and the devices connected to the other PoE ports.

Cisco Universal Power Over Ethernet

Cisco Universal Power Over Ethernet (Cisco UPOE) is a Cisco proprietary technology that extends the IEEE 802.3 at PoE standard to provide the capability to source up to 60 W of power over standard Ethernet cabling infrastructure (Class D or better) by using the spare pair of an RJ-45 cable (wires 4,5,7,8) with the signal pair (wires 1,2,3,6). Power on the spare pair is enabled when the switch port and end device mutually identify themselves as Cisco UPOE-capable using CDP or LLDP and the end device requests for power to be enabled on the spare pair. When the spare pair is powered, the end device can negotiate up to 60 W of power from the switch using CDP or LLDP.

If the end device is PoE-capable on both signal and spare pairs but does not support the CDP or LLDP extensions required for Cisco UPOE, a 4-pair forced mode configuration automatically enables power on both signal and spare pairs from the switch port.

Related Topics

[Supported Protocols and Standards](#), on page 87

How to Configure PoE and UPoE

Configuring a Power Management Mode on a PoE Port



Note

When you make PoE configuration changes, the port being configured drops power. Depending on the new configuration, the state of the other PoE ports, and the state of the power budget, the port might not be powered up again. For example, port 1 is in the auto and on state, and you configure it for static mode. The device removes power from port 1, detects the powered device, and repowers the port. If port 1 is in the auto and on state and you configure it with a maximum wattage of 10 W, the device removes power from the port and then redetects the powered device. The device repowers the port only if the powered device is a class 1, class 2, or a Cisco-only powered device.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet2/0/1	Specifies the physical port to be configured, and enters interface configuration mode.
Step 4	power inline {auto [<i>max max-wattage</i>] never static [<i>max max-wattage</i>] consumption <i>milli-watts-consumption</i>} Example: Device(config-if)# power inline auto	Configures the PoE mode on the port. The keywords have these meanings: <ul style="list-style-type: none"> • auto—Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. This is the default setting. • max <i>max-wattage</i>—Limits the power allowed on the port. The range for Cisco UPOE ports is 4000 to 60000 mW. If no value is specified, the maximum is allowed. • never—Disables device detection, and disable power to the port.

	Command or Action	Purpose
		<p>Note If a port has a Cisco powered device connected to it, do not use the power inline never command to configure the port. A false link-up can occur, placing the port into the error-disabled state.</p> <ul style="list-style-type: none"> • static—Enables powered-device detection. Pre-allocate (reserve) power for a port before the device discovers the powered device. The device reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection. • consumption —Sets the PoE consumption (in milliwatts) of the powered device connected to a specific interface. The power consumption can range from 4000 to 60000 milliWatts. <p>To reenable the automatic adjustment of consumption, either use the no keyword or specify 60000 milliwatts</p> <p>The device allocates power to a port configured in static mode before it allocates power to a port configured in auto mode.</p>
Step 5	end Example: Device(config-if) # end	Returns to privileged EXEC mode.
Step 6	show power inline [<i>[interface-id]</i> [detail]] Example: Device# show power inline	Displays PoE status for a device , for the specified interface.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Enabling Power on Signal/Spare Pairs



Note Do not enter this command if the end device cannot source inline power on the spare pair or if the end device supports the CDP or LLDP extensions for Cisco UPOE.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet2/0/1	Specifies the physical port to be configured, and enters interface configuration mode.
Step 3	power inline four-pair forced Example: Device(config-if)# power inline four-pair forced	Enables power on both signal and spare pairs from a switch port.
Step 4	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Configuring Power Policing

By default, the device monitors the real-time power consumption of connected powered devices. You can configure the device to police the power usage. By default, policing is disabled.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet2/0/1	Specifies the physical port to be configured, and enter interface configuration mode.
Step 4	power inline police [action {log errdisable}] Example: Device(config-if)# power inline police	<p>If the real-time power consumption exceeds the maximum power allocation on the port, configures the device to take one of these actions:</p> <ul style="list-style-type: none"> • power inline police—Shuts down the PoE port, turns off power to it, and puts it in the error-disabled state. <p>Note You can enable error detection for the PoE error-disabled cause by using the errdisable detect cause inline-power global configuration command. You can also enable the timer to recover from the PoE error-disabled state by using the errdisable recovery cause inline-power interval <i>interval</i> global configuration command.</p> <ul style="list-style-type: none"> • power inline police action errdisable—Turns off power to the port if the real-time power consumption exceeds the maximum power allocation on the port. • power inline police action log—Generates a syslog message while still providing power to the port. <p>If you do not enter the action log keywords, the default action shuts down the port and puts the port in the error-disabled state.</p>
Step 5	exit Example: Device(config-if)# exit	Returns to global configuration mode.
Step 6	Use one of the following: <ul style="list-style-type: none"> • errdisable detect cause inline-power • errdisable recovery cause inline-power • errdisable recovery interval <i>interval</i> 	(Optional) Enables error recovery from the PoE error-disabled state, and configures the PoE recover mechanism variables. By default, the recovery interval is 300 seconds.

	Command or Action	Purpose
	Example: <pre>Device(config)# errdisable detect cause inline-power</pre> <pre>Device(config)# errdisable recovery cause inline-power</pre> <pre>Device(config)# errdisable recovery interval 100</pre>	For interval <i>interval</i> , specifies the time in seconds to recover from the error-disabled state. The range is 30 to 86400.
Step 7	exit Example: <pre>Device(config)# exit</pre>	Returns to privileged EXEC mode.
Step 8	Use one of the following: <ul style="list-style-type: none"> • show power inline police • show errdisable recovery Example: <pre>Device# show power inline police</pre> <pre>Device# show errdisable recovery</pre>	Displays the power monitoring status, and verify the error recovery settings.
Step 9	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Monitoring Power Status

Table 15: Show Commands for Power Status

Command	Purpose
show power inline police	Displays the power policing data.
show power inline <i>[[interface-id] [detail]]</i>	Displays PoE status for an interface on a switch.
show power inline consumption <i>interface-id</i>	Displays the POE consumption for that interface.

Additional References for PoE

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for Power over Ethernet

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.6.1	Power over Ethernet (PoE)	<p>Power over Ethernet (PoE) allows the LAN switching infrastructure to provide power to an endpoint, called a powered device, over a copper Ethernet cable. The following types of end points can be powered through PoE:</p> <ul style="list-style-type: none">• A Cisco prestandard powered device• An IEEE 802.3af-compliant powered device• An IEEE 802.3at-compliant powered device

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 10

Configuring EEE

- [Restrictions for EEE, on page 99](#)
- [Information About EEE, on page 99](#)
- [How to Configure EEE, on page 100](#)
- [Monitoring EEE, on page 101](#)
- [Configuration Examples for Configuring EEE, on page 101](#)
- [Additional References for EEE, on page 102](#)
- [Feature History for Configuring EEE, on page 102](#)

Restrictions for EEE

EEE has the following restrictions:

- Changing the EEE configuration resets the interface because the device has to restart Layer 1 autonegotiation.
- You might want to enable the Link Layer Discovery Protocol (LLDP) for devices that require longer wakeup times before they are able to accept data on their receive paths. Doing so enables the device to negotiate for extended system wakeup times from the transmitting link partner.

Information About EEE

EEE Overview

Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods.

EEE can be enabled on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

Default EEE Configuration

How to Configure EEE

You can enable or disable EEE on an interface that is connected to an EEE-capable link partner.

Enabling or Disabling EEE

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet1/0/1	Specifies the interface to be configured, and enter interface configuration mode.
Step 3	power efficient-ethernet auto Example: Device(config-if)# power efficient-ethernet auto	Enables EEE on the specified interface. When EEE is enabled, the device advertises and autonegotiates EEE to its link partner.
Step 4	no power efficient-ethernet auto Example: Device(config-if)# no power efficient-ethernet auto	Disables EEE on the specified interface.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example:	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	Device# copy running-config startup-config	

Monitoring EEE

Table 16: Commands for Displaying EEE Settings

Command	Purpose
show eee capabilities interface <i>interface-id</i>	Displays EEE capabilities for the specified interface.
show eee status interface <i>interface-id</i>	Displays EEE status information for the specified interface.
show eee counters interface <i>interface-id</i>	Displays EEE counters for the specified interface.

Following are examples of the **show eee** commands

```
Switch#show eee capabilities interface gigabitEthernet 2/0/1
Gi2/0/1
EEE(efficient-ethernet): yes (100-Tx and 1000T auto)
Link Partner : yes (100-Tx and 1000T auto)
```

```
ASIC/Interface : EEE Capable/EEE Enabled
```

```
Switch#show eee status interface gigabitEthernet 2/0/1
Gi2/0/1 is up
EEE(efficient-ethernet): Operational
Rx LPI Status : Low Power
Tx LPI Status : Low Power
Wake Error Count : 0
```

```
ASIC EEE STATUS
Rx LPI Status : Receiving LPI
Tx LPI Status : Transmitting LPI
Link Fault Status : Link Up
Sync Status : Code group synchronization with data stream intact
```

```
Switch#show eee counters interface gigabitEthernet 2/0/1
```

```
LP Active Tx Time (10us) : 66649648
LP Transitioning Tx : 462
LP Active Rx Time (10us) : 64911682
LP Transitioning Rx : 153
```

Configuration Examples for Configuring EEE

This example shows how to enable EEE for an interface:

```
Device# configure terminal
Device(config)# interface gigabitEthernet1/0/1
```

```
Device(config-if)# power efficient-ethernet auto
```

This example shows how to disable EEE for an interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no power efficient-ethernet auto
```

Additional References for EEE

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for Configuring EEE

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.6.1	Energy Efficient Ethernet	Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 11

M2 SATA Module on Cisco Catalyst 9400 Series Supervisor

- [M2 SATA Module on Cisco Catalyst 9400 Series Supervisor, on page 105](#)
- [File System and Storage on M2 SATA, on page 105](#)
- [Accessing File System on M2 SATA, on page 106](#)
- [Formatting the M2 SATA Flash Disk, on page 106](#)
- [Operations on the SATA Module, on page 106](#)
- [Feature History and Information for M2 SATA Module, on page 107](#)

M2 SATA Module on Cisco Catalyst 9400 Series Supervisor

Cisco Catalyst 9400 is a next generation modular switch that supports model-driven programmability, streaming telemetry, and so on. To support the storage need for these features, the Cisco Catalyst 9400 Series Supervisor has an M2 connector that hosts a 22x88mm M2 SATA flash card. SATA configuration ranges from 240GB, 480GB to 960GB.

File System and Storage on M2 SATA

Cisco IOS XE 16.6.1 uses only partition 1 on the M2 SATA. If there is no file system present on partition 1 of the M2 card, the Cisco IOS XE 16.6.1 software creates a Linux ext2 filesystem (Linux ext2 is a standard Linux filesystem designed for generic block devices). Each time the device boots, the filesystem on partition 1 is checked. If any repairs are needed, they are made automatically. But if the filesystem is not in the “ext2” format or is unrepairable, a new ext2 filesystem is created and all existing data becomes unreadable or unrecoverable.

- Files stored on the M2 SATA partition are compatible with files stored on other devices.
- You can copy, or, store files between M2 SATA and other types of devices such as USB, eUSB, flash, and other IOS-XE file-system or storage.
- M2 SATA supports different types of storage access such as block-byte; read-store-modify.

Accessing File System on M2 SATA

The mounted file system from the M2 flash card is accessed at disk0: .

Copying files to and from bootflash: or usbflash0: is supported.

Formatting the M2 SATA Flash Disk

To format a new Flash Disk, use the **format disk0:** command.

The format command recursively deletes all files on the device. This command fails if any file is open during its execution.

```
Switch# format disk0:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "disk0:". Continue? [confirm]
Format of disk0: complete
```

Operations on the SATA Module

The following are some of the operations that you can perform on the SATA:

- dir
- copy
- delete
- show disk0:
- show file information disk0:
- show file systems

Following are sample outputs of the operations:

```
Switch# dir disk0:
Directory of disk0:/
 11  drwx           16384  Jul 13 2017 14:51:08 +00:00  lost+found
 13  -rw-           17866  Aug 11 2017 09:51:22 +00:00  test.txt
118148280320 bytes total (112084099072 bytes free)
```

Copy a file from the disk0: to USB

```
Switch# copy disk0:test.txt usbflash0:
Destination filename [test.txt]?
Copy in progress...C
17866 bytes copied in 0.096 secs (186104 bytes/sec)
```

```
Switch# dir usbflash0:
Directory of usbflash0:/
 12  -rw-          33554432  Jul 28 2017 10:12:58 +00:00  nvram_config
 11  drwx           16384  Jul 28 2017 10:09:46 +00:00  lost+found
 13  -rw-           17866  Aug 11 2017 09:52:16 +00:00  test.txt
189628416 bytes total (145387520 bytes free)
```

Delete the file test.txt from disk0:

```

Switch# delete disk0:test.txt
Delete filename [test.txt]?
Delete disk0:/test.txt? [confirm]

Switch# dir disk0:
Directory of disk0:/
No files in directory
118148280320 bytes total (112084135936 bytes free)

Copy file test.txt from USB to disk0:

Switch# copy usbflash0:test.txt disk0:
Destination filename [test.txt]?
Copy in progress...C
17866 bytes copied in 0.058 secs (308034 bytes/sec)

Switch# dir disk0:
Directory of disk0:/
  11  -rw-                17866  Aug 11 2017 09:53:03 +00:00  test.txt
118148280320 bytes total (112084115456 bytes free)

```

Show commands

```

Switch# show disk0:
-#- --length-- -----date/time----- path
   2      17866 Aug 11 2017 09:54:06.0000000000 +00:00 test.txt
112084115456 bytes available (62513152 bytes used)

Switch# show file information disk0:test.txt
disk0:test.txt:
  type is image (elf64) []
  file size is 448 bytes, run size is 448 bytes
Foreign image, entry point 0x400610

Switch# show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
      -         -         opaque  rw    system:
      -         -         opaque  rw    tmpsys:
* 11250098176    9694093312    disk   rw    bootflash: flash:
  1651314688    1232220160    disk   rw    crashinfo:
  118148280320  112084115456    disk   rw    disk0:
    189628416    145387520     disk   rw    usbflash0:
    7763918848    7696850944     disk   ro    webui:
      -         -         opaque  rw    null:
      -         -         opaque  ro    tar:
      -         -     network  rw    tftp:
    33554432     33532852     nvram   rw    nvram:
      -         -         opaque  wo    syslog:
      -         -     network  rw    rcp:
      -         -     network  rw    http:
      -         -     network  rw    ftp:
      -         -     network  rw    scp:
      -         -     network  rw    https:
      -         -         opaque  ro    cns:

```

Feature History and Information for M2 SATA Module

Release	Modification
Cisco IOS XE Everest 16.6.1	This feature was introduced.

