



CHAPTER 13

Configuring Interface Characteristics

This chapter defines the types of Catalyst 2960, 2960-S, and 2960-C interfaces and describes how to configure them. Unless otherwise noted, the term *switch* refers to a standalone switch and a switch stack.

- [Understanding Interface Types, page 13-1](#)
- [Using the Switch USB Ports, page 13-13](#)
- [Using Interface Configuration Mode, page 13-19](#)
- [Using the Ethernet Management Port \(Catalyst 2960-S Only\), page 13-24](#)
- [Configuring Ethernet Interfaces, page 13-27](#)
- [Configuring Layer 3 SVIs, page 13-41](#)
- [Configuring the System MTU, page 13-42](#)
- [Monitoring and Maintaining the Interfaces, page 13-44](#)



Note

For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the *Cisco IOS Interface Command Reference, Release 12.4* on Cisco.com.

Understanding Interface Types

This section describes the different types of supported interfaces with references to chapters that contain more detailed information about configuring these interfaces.



Note

The stack ports on the rear of the switch are not Ethernet ports and cannot be configured.

- [Port-Based VLANs, page 13-2](#)
- [Switch Ports, page 13-2](#)
- [Switch Virtual Interfaces, page 13-3](#)
- [EtherChannel Port Groups, page 13-4](#)
- [Dual-Purpose Uplink Ports, page 13-4](#)
- [Power over Ethernet Ports, page 13-5](#)
- [Connecting Interfaces, page 13-13](#)

Port-Based VLANs

**Note**

Stacking is supported only on Catalyst 2960-S switches running the LAN base image.

A VLAN is a switched network that is logically segmented by function, team, or application, without regard to the physical location of the users. For more information about VLANs, see the [Chapter 14, “Configuring VLANs.”](#) 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 you configure a local port 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, you must first set VTP mode to transparent to configure extended-range VLANs (VLAN IDs 1006 to 4094). Extended-range VLANs created in transparent mode are not added to the VLAN database but are saved in the switch running configuration. With VTP version 3, you can create extended-range VLANs in client or server mode. These VLANs are saved in the VLAN database.

VLANs can be formed with ports across the stack. The VLAN database is downloaded to all switches in a stack, and all switches in the stack build the same VLAN database. The running configuration and the saved configuration are the same for all switches in a stack.

**Note**

Stacking is supported only on Catalyst 2960-S switches running the LAN base image.

Add ports to a VLAN by using the **switchport** interface configuration commands:

- 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. You use switch ports for managing the physical interface and associated Layer 2 protocols.

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.

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

For detailed information about configuring access port and trunk port characteristics, see [Chapter 14, “Configuring VLANs.”](#)

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 an 802.1Q tagged packet, the packet is dropped, and the source address is not learned.

Supported access ports:

- Static access ports are manually assigned to a VLAN (or through a RADIUS server for use with IEEE 802.1x). For more information, see the [“802.1x Authentication with VLAN Assignment” section on page 12-17](#).
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is not a member of any VLAN. Traffic forwarding to and from the port is enabled only when the port VLAN membership is discovered. Dynamic access ports on the switch are assigned to a VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6500 series switch. The Catalyst 2960, 2960-S or 2960-C switch cannot be a VMPS server.

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. For more information about voice VLAN ports, see [Chapter 16, “Configuring Voice VLAN.”](#)

Trunk Ports

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

The switch supports only 802.1Q trunk ports. An 802.1Q trunk port supports simultaneous tagged and untagged traffic. The 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 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 affects only 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 enabled. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list, the trunk port automatically becomes a member of that VLAN. Traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of an enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and traffic for the VLAN is not forwarded to or from the port.

For more information about trunk ports, see [Chapter 14, “Configuring VLANs.”](#)

Switch Virtual Interfaces

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing or bridging 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 switch.

By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly configured.

**Note**

You cannot delete interface VLAN 1.

SVIs provide IP host connectivity only to the system. Beginning with Cisco IOS release 12.2(55)SE, you can enable routing and configure static routes on SVIs.

**Note**

Static routing is supported on SVIs only when the switch is running the LAN base image.

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 encapsulated trunk port 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. For more information, see the [“Manually Assigning IP Information”](#) section on page 3-14.

**Note**

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

EtherChannel Port Groups

EtherChannel port groups treat multiple switch ports as one switch port. An EtherChannel port group acts as a single logical port for high-bandwidth connections between switches or between switches 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 or multiple access ports into one logical access port. Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. The DTP, the Cisco Discovery Protocol (CDP), and the Port Aggregation Protocol (PAgP) operate only on physical ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel. Use the **channel-group** interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together.

For more information, see [Chapter 39, “Configuring EtherChannels and Link-State Tracking.”](#)

Dual-Purpose Uplink Ports

**Note**

Catalyst 2960-S switches do not have dual-purpose uplink ports.

Some switches support dual-purpose uplink ports. Each uplink port is considered as a single interface with dual front ends—an RJ-45 connector and a small form-factor pluggable (SFP) module connector. The dual front ends are not redundant interfaces, and the switch activates only one connector of the pair.

By default, the switch dynamically selects the interface type that first links up. However, you can use the **media-type** interface configuration command to manually select the RJ-45 connector or the SFP module connector. For information about configuring speed and duplex settings for a dual-purpose uplink, see the [“Setting the Interface Speed and Duplex Parameters”](#) section on page 13-31.

Each uplink port has two LEDs: one shows the status of the RJ-45 port, and one shows the status of the SFP module port. The port LED is on for whichever connector is active. For more information about the LEDs, see the hardware installation guide.

Power over Ethernet Ports



Note

PoE is supported only when the switch is running the LAN base image. Power over Ethernet Plus (PoE+) is supported only on Catalyst 2960-S switches.

PoE switch ports automatically supply power to these connected devices (if the switch senses that there is no power on the circuit):

- Cisco pre-standard powered devices (such as Cisco IP Phones and Cisco Aironet access points)
- IEEE 802.3 af-compliant powered devices
- IEEE 802.3 at-compliant powered devices (PoE+ on Catalyst 2960-S switches only)

A powered device can receive redundant power when it is connected only to a PoE switch port and to an AC power source. After the switch detects a powered device, it determines the device power requirements and then grants or denies power to the device. The switch can also sense the real-time power consumption of the device by monitoring and policing the power usage.

This section has this PoE information:

- [Supported Protocols and Standards, page 13-5](#)
- [Powered-Device Detection and Initial Power Allocation, page 13-6](#)
- [Power Management Modes, page 13-7](#)
- [Power Monitoring and Power Policing, page 13-8](#)

Supported Protocols and Standards

The switch uses these protocols and standards to support PoE:

- CDP with power consumption—The powered device notifies the switch of the amount of power it is consuming. The switch does not reply to the power-consumption messages. The switch can only supply power to or remove power from the PoE port.
- Cisco intelligent power management—The powered device and the switch negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-power Cisco powered device, which consumes more than 7 W, to operate at its highest power mode. The powered device first boots up in low-power mode, consumes less than 7 W, and negotiates to obtain enough power to operate in high-power mode. The device changes to high-power mode only when it receives confirmation from the switch.

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

Cisco intelligent power management is backward-compatible with CDP with power consumption; the switch responds according to the CDP message that it receives. CDP is not supported on third-party powered devices; therefore, the switch 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 —This PoE+ standard supports all the features of 802.1af and increases the maximum power available on each PoE port from 15.4 W to 30 W. The 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 Power-via-MDI TLV can provide power on the spare pair.

For more information about UPoE, see [Universal Power Over Ethernet, page 13-11](#).



Note Only Catalyst 2960-S or 2960-C switches support IEEE 802.3at.

Powered-Device Detection and Initial Power Allocation

The switch 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 switch determines the device power requirements based on its type:

- A Cisco prestandard powered device does not provide its power requirement when the switch detects it, so a switch that does not support PoE+ allocates 15.4 W as the initial allocation for power budgeting; a PoE+ switch allocates 30 W (PoE+).

The initial power allocation is the maximum amount of power that a powered device requires. The switch initially allocates this amount of power when it detects and powers the powered device. As the switch receives CDP messages from the powered device and as the powered device negotiates power levels with the switch through CDP power-negotiation messages, the initial power allocation might be adjusted.

- The switch classifies the detected IEEE device within a power consumption class. Based on the available power in the power budget, the switch determines if a port can be powered. [Table 13-1](#) lists these levels.

Table 13-1 IEEE Power Classifications

Class	Maximum Power Level Required from the Switch
0 (class status unknown)	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W PoE+ devices only

The switch monitors and tracks requests for power and grants power only when it is available. The switch tracks its power budget (the amount of power available on the switch for PoE). The switch 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 switch uses CDP to determine the *actual* power consumption requirement of the connected Cisco powered devices, and the switch adjusts the power budget accordingly. This does not apply to third-party PoE devices. The switch processes a request and either grants or denies power. If the request is granted, the switch updates the power budget. If the request is denied, the switch ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. Powered devices can also negotiate with the switch for more power.

If the switch 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.

In a Catalyst 2960-S switch stack, the PoE feature operates the same whether or not the switch is a stack member. The power budget is per-switch and independent of any other switch in the stack. Election of a new stack master does not affect PoE operation. The stack master keeps track of PoE status for all switches and ports in the stack and includes the status in output displays.

Power Management Modes

Supported PoE modes:

- **auto**—The switch automatically detects if the connected device requires power. If the switch discovers a powered device connected to the port and if the switch 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 switch has enough power for all the powered devices, they all come up. If enough power is available for all powered devices connected to the switch, 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 switch 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 switch periodically rechecks the power budget and continues to attempt to grant the request for power.

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

If a powered device is removed, the switch 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 switch does not provide power to the port. If the switch powers a powered device, but the powered device later requests through CDP messages more than the configured maximum value, the switch 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 switch delivers the maximum value. Use the **auto** setting on any PoE port. The auto mode is the default setting.

- **static**—The switch pre-allocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port. The switch 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 switch does not supply power to it. If the switch learns through CDP messages that the powered device needs more than the maximum wattage, the powered device is shutdown.

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

- **never**—The switch 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 power is never applied to a PoE-capable port, making the port a data-only port.

For information on configuring a PoE port, see the [“Configuring a Power Management Mode on a PoE Port” section on page 13-34](#).

Power Monitoring and Power Policing

When policing of the real-time power consumption is enabled, the switch 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 switch senses the real-time power consumption of the powered device and monitors the power consumption of the connected powered device; this is called *power monitoring* or *power sensing*. The switch also uses the *power policing* feature to police the power usage.

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. For more information about these PoE features, see the [“Powered-Device Detection and Initial Power Allocation” section on page 13-6](#).

The switch senses the power consumption of the connected device as follows:

1. The switch monitors the real-time power consumption on individual ports.
2. The switch records the power consumption, including peak power usage, and reports the information through an SNMP MIB, CISCO-POWER-ETHERNET-EXT-MIB.
3. If power policing is enabled, the switch polices power usage by comparing the real-time power consumption to the maximum power allocated to the device. For more information about the maximum power consumption, also referred to as the *cutoff power*, on a PoE port, see the [“Maximum Power Allocation \(Cutoff Power\) on a PoE Port” section on page 13-8](#).

If the device uses more than the maximum power allocation on the port, the switch can either turn off power to the port, or the switch 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 switch configuration. By default, power-usage policing is disabled on all PoE ports.

If error recovery from the PoE error-disabled state is enabled, the switch 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, no action occurs when the powered device consumes more than the maximum power allocation on the PoE port, which could adversely affect the switch.

Maximum Power Allocation (Cutoff Power) on a PoE Port

When power policing is enabled, the switch determines the cutoff power on the PoE port in this order:

1. Manually when you set the user-defined power level that the switch budgets for the port by using the **power inline consumption default** *wattage* global or interface configuration command

2. Manually when you set the user-defined power level that limits the power allowed on the port by using the **power inline auto max** *max-wattage* or the **power inline static max** *max-wattage* interface configuration command
3. Automatically when the switch sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation.

Use the first or second method in the previous list to manually configure the cutoff-power value by entering the **power inline consumption default** *wattage* or the **power inline [auto | static max]** *max-wattage* command. If you do not manually configure the cutoff-power value, the switch automatically determines the value by using CDP power negotiation. If the switch cannot determine the value by using one of these methods, it uses the default value of 15.4 W.

On a switch with PoE+, if you do not manually configure the cutoff-power value, the switch automatically determines it by using CDP power negotiation or the device IEEE classification and LLDP power negotiation. If CDP or LLDP are not enabled, the default value of 30 W is applied. However without CDP or LLDP, the switch does not allow devices to consume more than 15.4 W of power because values from 15400 to 30000 mW are only allocated based on CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device might be in violation of the maximum current (*I_{max}*) limitation and might experience an *I_{cut}* fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

**Note**

When a powered device connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the switch locks to the power-negotiation protocol of that first packet and does not respond to power requests from the other protocol. For example, if the switch is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the switch has locked on it, the switch does not respond to LLDP power requests and can no longer power on any accessories. In this case, you should restart the powered device.

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 switch 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 switch uses for power policing is not equal to the configured power value.

When power policing is enabled, the switch 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.

The actual amount of power consumed by a powered device on a PoE port is the cutoff-power value plus a calibration factor of 500 mW (0.5 W). The actual cutoff value is approximate and varies from the configured value by a percentage of the configured value. For example, if the configured cutoff power is 12 W, the actual cutoff-value is 11.4 W, which is 0.05% less than the configured value.

We recommend that you enable power policing when PoE is enabled on your switch. For example, 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 switch 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 switch does not provide power to the connected device. After the switch turns on power to the

PoE port, the switch 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 switch and the devices connected to the other PoE ports.

Because the switch supports internal power supplies and the Cisco Redundant Power System 2300 (also referred to as the RPS 2300), the total amount of power available for the powered devices varies depending on the power supply configuration.

- If a power supply is removed and replaced by a new power supply with less power and the switch does not have enough power for the powered devices, the switch denies power to the PoE ports that are in auto mode in descending order of the port numbers. If the switch still does not have enough power, it denies power to the PoE ports in static mode in descending order of the port numbers.
- If the new power supply supports more power than the previous one and the switch now has more power available, the switch grants power to the PoE ports in static mode in ascending order of the port numbers. If it still has power available, the switch then grants power to the PoE ports in auto mode in ascending order of the port numbers.

For configuration information, see the [“Configuring Power Policing”](#) section on page 13-37.

PoE Uplinks and PoE Pass-Through Capability

The Catalyst 2960-C compact switch can receive power on the two uplink Gigabit Ethernet ports from a PoE or PoE+ capable-switch (for example a Catalyst 3750-X or 3560-X switch). The switch can also receive power from an AC power source when you use the auxiliary power input. When both uplink ports and auxiliary power are connected, the auxiliary power input takes precedence.

The Catalyst 2960CPD-8PT switch can provide power to end devices through the eight downlink ports in one of two ways:

- When the switch receives power from the auxiliary power input, it acts like any other PoE switch and can supply power to end devices connected to the eight downlink ports according to the total power budget. Possible end devices are IP phones, video cameras, and access points.
- When the switch receives power through one or both uplink ports, it can provide PoE pass-through, taking the surplus power from the PoE or PoE+ uplinks and passing it through the downlink ports to end devices. The available power depends on the power drawn from the uplink ports and varies, depending if one or both uplink ports are connected and if the source is PoE or PoE+.

The downlink ports are PoE-capable, and each port can supply up to 15.4 W per port to a connected powered device. When the switch draws power from the uplink ports, the power budget (the available power on downlink ports) depends on the power source options shown in the table. When the switch receives power through the auxiliary connector, the power budget is similar to that of any other PoE switch.

Table 13-2 Catalyst 2960CPD-8PT Power Budget

Power Source Options	Power Sent from Uplink Switches	Available PoE Budget
1 PoE uplink port	15.4 W	0
2 PoE uplink ports	30.8 W	7 W
1 PoE+ uplink port	30 W	7 W
1 PoE and 1 PoE+ uplink	45.4 W	15.4 W
2 PoE+ uplink ports	60 W	22.4 W
Auxiliary power input	—	22.4 W

For information about configuring these ports, see the “[Configuring Catalyst PoE and PoE Pass-Through Ports on Compact Switches](#)” section on page 13-39.

Universal Power Over Ethernet



Note Only Catalyst 2960-C switches support Universal Power over Ethernet.

Universal Power over Ethernet (UPoE) is a Cisco proprietary technology that extends the IEEE 802.3at PoE standard to provide the capability to source up to 60 W of power over standard Ethernet cabling infrastructure (Class D or better). The 3K-X UPoE capabilities provide up to 60 W 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 enddevice mutually identify themselves as Universal PoE (UPoE)-capable using CDP or LLDP and the enddevice requests for power to be enabled on the spare pair. When the spare pair is powered, the enddevice can negotiate up to 60 W of power from the switch using CDP or LLDP.

Enabling Power on Signal/Spare Pairs

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

To enable the power on the pairs, follow these steps:

	Command	Purpose
Step 1	interface terminal	Changes the mode to global configuration.
Step 2	interface {fastethernet gigabitethernet} slot/port	Selects the interface to configure.
Step 3	[no] power inline four-pair forced	Automatically enables or disables power on both signal and spare pairs from a switch port.
Step 4	end	Exits configuration mode.
Step 5	show platform software interface {fastethernet gigabitethernet} slot/port status	Displays EEE status.

The following example shows how to automatically enable power on both signal and spare pairs from switch port Gigabit Ethernet 2/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# power inline four-pair forced
Switch(config-if)# end
```



Note Do not enter this command if the enddevice cannot source inline power on the spare pair or if the enddevice supports the CDP or LLDP extensions for UPoE.

Configuring Power Consumption for Powered Devices on an Interface

When the switch detects a powered device on an interface, it provides the default power to the device. When the switch receives a CDP packet from the powered device, the power is automatically negotiated to a wattage required by the device. Normally, this automatic negotiation works well, and no further configuration is required or recommended. However, you can specify the powered device's consumption for a particular interface to provide extra functionality from your switch. This operation is useful when CDP is disabled or not available.

To change the power consumption of a single powered device, follow these steps:

	Command	Purpose
Step 1	<code>interface {fastethernet gigabitethernet} slot/port</code>	Selects the interface to configure.
Step 2	<code>[no] power inline consumption milli-watts</code>	Sets the PoE consumption (in milliwatts) of the powered device connected to a specific interface. The power consumption can range from 4000 to 60000. To reenble the automatic adjustment of consumption, use the no keyword.
Step 3	<code>end</code>	Exits configuration mode.
Step 4	<code>show power inline consumption {fastethernet gigabitethernet} slot/port</code>	Displays the PoE consumption for the interface.

At a given time, you can use only one of the power negotiation protocols between CDP and LLDP. The following examples show how to enable or disable the power negotiation protocols:

```
Switch(config)# [no] lldp run
Switch(config)# [no] cdp run
```



Note

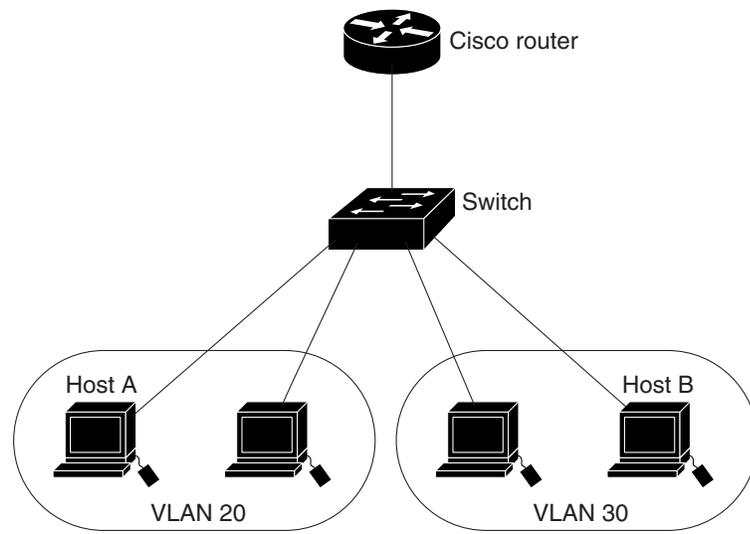
The Power Device (PD) and Power Source Equipment (PSE) should run the same power negotiation protocol to negotiate power.

Connecting Interfaces

Devices within a single VLAN can communicate directly through any switch. Ports in different VLANs cannot exchange data without going through a routing device.

In the configuration shown in [Figure 13-1](#), when Host A in VLAN 20 sends data to Host B in VLAN 30, the data must go from Host A to the switch, to the router, back to the switch, and then to Host B.

Figure 13-1 Connecting VLANs with Layer 2 Switches



With a standard Layer 2 switch, ports in different VLANs have to exchange information through a router. By using the switch 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 switch with no need for an external router ([Figure 13-1](#)).

Using the Switch USB Ports



Note

USB ports are supported only on Catalyst 2960-S and 2960-C switches.

The Catalyst 2960-S and Catalyst 2960-C Gigabit Ethernet switches have two USB ports on the front panel:

- [USB Mini-Type B Console Port, page 13-14](#)
- [USB Type A Port, page 13-16](#)

The Catalyst Fast Ethernet switches (Catalyst 2960CPD-8PT-L and the 2960CPD-8TT-L switches) have only the USB mini-Type B console port.

USB Mini-Type B Console Port

The switch has two console ports available—a USB mini-Type B console connection and an 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. 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 switch. The connected device must include a terminal emulation application. When the switch 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 switch 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 switch always first displays the RJ-45 media type. Each switch in a 2960-S stack issues this log.

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

```
switch-stack-1
*Mar  1 00:01:00.171: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
*Mar  1 00:01:00.431: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.

switch-stack-2
*Mar  1 00:01:09.835: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
switch-stack-3)
*Mar  1 00:01:10.523: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

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

```
switch-stack-1
Mar  1 00:20:48.635: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

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

Configuring the Console Media Type

Beginning in privileged EXEC mode, follow these steps to select the RJ-45 console media type. If you configure the RJ-45 console, USB console operation is disabled, and input always remains with the RJ-45 console.

This configuration applies to all switches in a stack.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	line console 0	Configure the console. Enter line configuration mode.
Step 3	media-type rj45	Configure the console media type to always be RJ-45. If you do not enter this command and both types are connected, the default is USB.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-configuration	Verify your settings.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example disables the USB console media type and enables the RJ-45 console media type.

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# media-type rj45
```

This configuration terminates any active USB console media type in the stack. A log shows that this termination has occurred. This example shows that the console on switch 1 reverted to RJ-45.

```
*Mar 1 00:25:36.860: %USB_CONSOLE-6-CONFIG_DISABLE: Console media-type USB disabled by
system configuration, media-type reverted to RJ45.
```

At this point no switches in the stack allow a USB console to have input. A log entry shows when a console cable is attached. If a USB console cable is connected to switch 2, it is prevented from providing input.

```
*Mar 1 00:34:27.498: %USB_CONSOLE-6-CONFIG_DISALLOW: Console media-type USB is disallowed
by system configuration, media-type remains RJ45. (switch-stk-2)
```

This example reverses the previous configuration and immediately activates any USB console that is connected.

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# no media-type rj45
```

Configuring the 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.



Note

The configured inactivity timeout applies to all switches in a stack. However, a timeout on one switch does *not* cause a timeout on other switches in the stack.

Beginning in privileged EXEC mode, follow these steps to configure an inactivity timeout.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	line console 0	Configure the console port. Enter console line configuration mode.
Step 3	usb-inactivity-timeout <i>timeout-minutes</i>	Specify an inactivity timeout for the console port. The range is 1 to 240 minutes. The default is to have no timeout configured.
Step 4	show running-configuration	Verify your setting.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example configures the inactivity timeout to 30 minutes:

```
Switch# configure terminal
Switch#(config)# line console 0
Switch#(config-line)# usb-inactivity-timeout 30
```

To disable the configuration, use these commands:

```
Switch#(config)# line console 0
Switch#(config-line)# no usb-inactivity-timeout
```

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.
```

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 switch supports Cisco 64 MB, 256 MB, 512 MB and 1 GB flash drives. 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 switch to boot from the USB flash drive.

Beginning in privileged EXEC mode, follow these steps to allow booting from the USB flash device.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	boot system flash usbflash0: <i>image</i>	Configure the switch to boot from the USB flash device. The <i>image</i> is the name of the bootable image.
Step 3	show running-configuration	Verify your setting.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To get information about the USB device, use the **show usb {controllers | device | driver | port | tree}** privileged EXEC command.

This example configures the switch to boot from the Catalyst 2960-S flash device. The image is the Catalyst 2960-S LAN base image.

```
Switch# configure terminal  
Switch#(config)# boot system flash usbflash0: c2960s-lanbase-mz
```

To disable booting from flash, enter the **no** form of the command.

This is sample output from the **show usb device** command:

```
Switch# show usb device  
Host Controller: 1  
Address: 0x1  
Device Configured: YES  
Device Supported: YES  
Description: STEC USB 1GB  
Manufacturer: STEC  
Version: 1.0  
Serial Number: STI 3D508232204731  
Device Handle: 0x1010000  
USB Version Compliance: 2.0  
Class Code: 0x0  
Subclass Code: 0x0  
Protocol: 0x0  
Vendor ID: 0x136b  
Product ID: 0x918  
Max. Packet Size of Endpoint Zero: 64  
Number of Configurations: 1  
Speed: High  
Selected Configuration: 1  
Selected Interface: 0  
  
Configuration:  
  Number: 1  
  Number of Interfaces: 1  
  Description: Storage  
  Attributes: None  
  Max Power: 200 mA  
  
  Interface:  
    Number: 0  
    Description: Bulk  
    Class Code: 8  
    Subclass: 6  
    Protocol: 80  
    Number of Endpoints: 2  
  
    Endpoint:  
      Number: 1  
      Transfer Type: BULK  
      Transfer Direction: Device to Host  
      Max Packet: 512  
      Interval: 0  
  
    Endpoint:  
      Number: 2  
      Transfer Type: BULK  
      Transfer Direction: Host to Device  
      Max Packet: 512  
      Interval: 0
```

This is sample output from the **show usb port** command:

```
Switch# show usb port  
Port Number: 0  
Status: Enabled  
Connection State: Connected  
Speed: High  
Power State: ON
```

Using Interface Configuration Mode

The switch supports these interface types:

- Physical ports—switch ports
- VLANs—switch virtual interfaces
- Port channels—EtherChannel interfaces

You can also configure a range of interfaces (see the “[Configuring a Range of Interfaces](#)” section on page 13-21).

To configure a physical interface (port) on a Catalyst 2960 or 2960-C switch or a Catalyst 2960-S switch running the LAN Lite image, specify the interface type, module number, and switch port number, and enter interface configuration mode. To configure a port on a Catalyst 2960-S switch running the LAN base image (supporting stacking), specify the interface type, stack member number, module number, and switch port number, and enter interface configuration mode.

- Type—Port types depend on those supported on the switch. Possible types are: Fast Ethernet (fastethernet or fa) for 10/100 Mb/s Ethernet, Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000 Mb/s Ethernet ports, 10-Gigabit Ethernet (tengigabitethernet or te) for 10,000 Mb/s, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces.
- Stack member number—The number that identifies the switch within the stack. The switch number range is 1 to 4 and is assigned the first time the switch initializes. The default switch number, before it is integrated into a switch stack, is 1. When a switch has been assigned a stack member number, it keeps that number until another is assigned to it.

You can use the switch port LEDs in Stack mode to identify the stack member number of a switch.

- Module number—The module or slot number on the switch (always 0).
- Port number—The interface number on the switch. The port numbers always begin at 1, starting with the far left port when facing the front of the switch, for example, gigabitethernet1/0/1. For a switch with 10/100/1000 ports and SFP module ports, SFP module ports are numbered consecutively following the 10/100/1000 ports.

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

These examples identify interfaces on a Catalyst 2960-S switch running the LAN base image:

- To configure 10/100/1000 port 4 on a standalone switch, enter this command:

```
Switch(config)# interface gigabit  
tethernet1/0/4
```

- To configure 10/100 port 4 on stack member 3, enter this command:

```
Switch(config)# interface gigabitethernet3/0/4
```

This example identifies an interface on a Catalyst 2960 or 2960-C switch or a Catalyst 2960-S switch running the LAN Lite image:

- To configure 10/100/1000 port 4, enter this command:

```
Switch(config)# interface gigabitethernet0/4
```



Note

Configuration examples and outputs in this book might not be specific to your switch, particularly regarding the presence of a stack member number.

Procedures for Configuring Interfaces

These general instructions apply to all interface configuration processes.

Step 1 Enter the **configure terminal** command at the privileged EXEC prompt:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Step 2 Enter the **interface** global configuration command.

Identify the interface type, the switch number, and the interface number. In this example, Gigabit Ethernet port 1 on switch 1 is selected:

Identify the interface type and the interface number, Gigabit Ethernet port 1 in this example:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)#
```



Note Entering a space between the interface type and interface number is optional

Step 3 Follow each **interface** command with the configuration commands that the interface requires. The commands that you enter define the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you enter another interface command or enter **end** to return to privileged EXEC mode.

You can also configure a range of interfaces by using the **interface range** or **interface range macro** global configuration commands. Interfaces configured in a range must be the same type and must be configured with the same feature options.

Step 4 After you configure an interface, verify its status by using the **show** privileged EXEC commands listed in the [“Monitoring and Maintaining the Interfaces”](#) section on page 13-44.

Enter the **show interfaces** privileged EXEC command to see 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.

Configuring a Range of Interfaces

You can use the **interface range** global configuration command to configure multiple interfaces with the same configuration parameters. 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.

Beginning in privileged EXEC mode, follow these steps to configure a range of interfaces with the same parameters:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface range { <i>port-range</i> macro <i>macro_name</i> }	Specify 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 “Configuring and Using Interface Range Macros” section on page 13-22. 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.
Step 3		Use the normal configuration commands to apply the configuration parameters to all interfaces in the range. Each command is executed as it is entered.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interfaces [<i>interface-id</i>]	Verify the configuration of the interfaces in the range.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

When using the **interface range** global configuration command, note these guidelines:

- Valid entries for *port-range*, depending on port types on the switch:
 - vlan** *vlan-ID*, where the VLAN ID is 1 to 4094



Note Although the command-line interface shows options to set multiple VLANs, these options are not supported on Catalyst 2960 and 2960-S switches.

- gigabitethernet** stack member/module/{*first port*} - {*last port*}, where the module is always 0
- fastethernet** module/{*first port*} - {*last port*}, where the module is always 0
- gigabitethernet** module/{*first port*} - {*last port*}, where the module is always 0
- port-channel** *port-channel-number* - *port-channel-number*, where the *port-channel-number* is 1 to 6



Note When you use the **interface range** command with port channels, the first and last port-channel number must be active port channels.

- You must add a space between the first interface number and the hyphen when using the **interface range** command.

For example, **interface range gigabitethernet1/0/1 - 4** is a valid range; **interface range gigabitethernet1/0/1-4** is not.

For example, **interface range gigabitethernet 0/1 - 4** is a valid range; **interface range gigabitethernet0/1-4** is not.

- The **interface range** command only works with VLAN interfaces that have been configured with the **interface vlan** command. The **show running-config** privileged EXEC command displays the configured VLAN interfaces. VLAN interfaces not displayed by the **show running-config** command cannot be used with the **interface range** command.
- All interfaces defined in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs), but you can enter multiple ranges in a command.

This example shows how to use the **interface range** global configuration command to set the speed on ports 1 to 2 to 100 Mb/s:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 2
Switch(config-if-range)# speed 100
```

This example shows how to use a comma to add different interface type strings to the range to enable Fast Ethernet ports 1 to 3 on switch 1 and Gigabit Ethernet ports 1 and 2 on switch 2 to receive flow-control pause frames:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 3, gigabitethernet1/0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

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

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.

Beginning in privileged EXEC mode, follow these steps to define an interface range macro:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	define interface-range <i>macro_name</i> <i>interface-range</i>	Define 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.

	Command	Purpose
Step 3	<code>interface range macro macro_name</code>	Select 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 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>show running-config include define</code>	Show the defined interface range macro configuration.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the **no define interface-range** *macro_name* global configuration command to delete a macro.

When using the **define interface-range** global configuration command, note these guidelines:

- Valid entries for *interface-range*, depending on port types on the switch:
 - vlan** *vlan-ID*, where the VLAN ID is 1 to 4094



Note Although the command-line interface shows options to set multiple VLANs, these options are not supported on Catalyst 2960 switches.

- fastethernet** stack member/module/{*first port*} - {*last port*}, where the module is always 0
- gigabitethernet** stack member/module/{*first port*} - {*last port*}, where the module is always 0
- fastethernet** module/{*first port*} - {*last port*}, where the module is always 0
- gigabitethernet** module/{*first port*} - {*last port*}, where the module is always 0
- port-channel** *port-channel-number* - *port-channel-number*, where the *port-channel-number* is 1 to 6



Note When you use the **interface range** command with port channels, the first and last port-channel number must be active port channels.

- You must add a space between the first interface number and the hyphen when entering an *interface-rang*.
For example, **gigabitethernet1/0/1 - 4** is a valid range; **gigabitethernet1/0/1-4** is not.
- The VLAN interfaces must have been configured with the **interface vlan** command. The **show running-config** privileged EXEC command displays the configured VLAN interfaces. VLAN interfaces not displayed by the **show running-config** command cannot be used as *interface-ranges*.
- All interfaces defined as in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs), but you can combine multiple interface types in a macro.

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

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet1/0/1 - 2
Switch(config)# end
Switch# show running-config | include define
Switch# define interface-range enet_list gigabitethernet1/0/1 - 2
```

This example shows how to create a multiple-interface macro named *macro1*:

```
Switch# configure terminal
Switch(config)# define interface-range macro1 gigabitethernet1/0/1 - 2,
gigabitethernet1/0/1 - 2
Switch(config)# end
```

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

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

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

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

Using the Ethernet Management Port (Catalyst 2960-S Only)



Note

The Ethernet management port is not supported on Catalyst 2960 switches.

- [Understanding the Ethernet Management Port, page 13-24](#)
- [Supported Features on the Ethernet Management Port, page 13-25](#)
- [Configuring the Ethernet Management Port, page 13-26](#)
- [TFTP and the Ethernet Management Port, page 13-26](#)

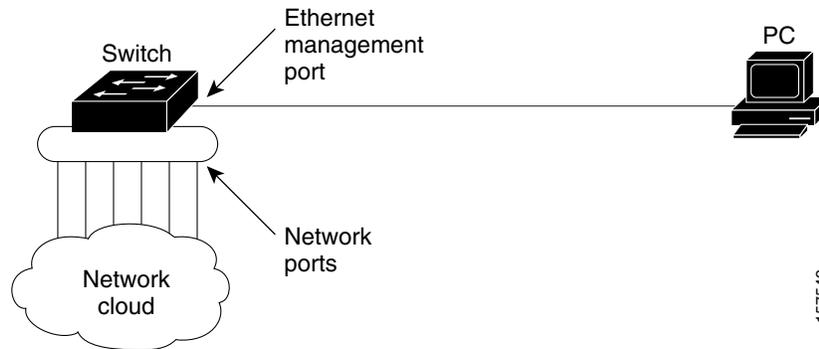
Understanding the Ethernet Management Port

The Ethernet management port, also referred to as the *Fa0* or *fastethernet0* port, is a Layer 3 host port to which you can connect a PC. You can use the Ethernet management port instead of the switch console port for network management. When managing a switch stack, connect the PC to the Ethernet management port on a Catalyst 2960-S stack member.

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

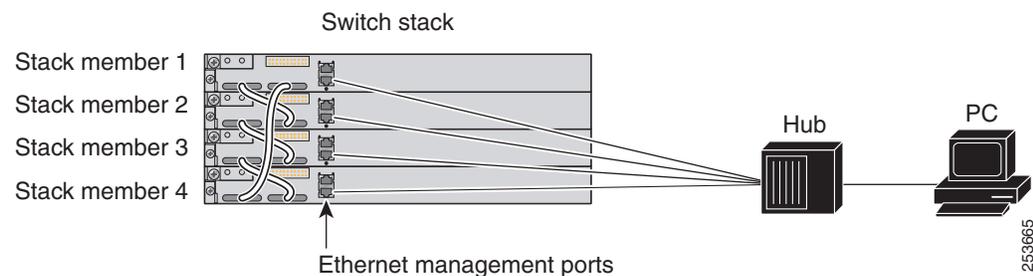
For a Catalyst 2960-S standalone switch, connect the Ethernet management port to the PC as shown in Figure 13-2.

Figure 13-2 Connecting a Switch to a PC



In a Catalyst 2960-S stack, all the Ethernet management ports on the stack members are connected to a hub to which the PC is connected. As shown in Figure 13-3, the active link is from the Ethernet management port on the stack master (switch 2) through the hub, to the PC. If the stack master fails and a new stack master is elected, the active link is now from the Ethernet management port on the new stack master to the PC.

Figure 13-3 Connecting a Switch Stack to a PC



By default, the Ethernet management port is enabled.

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)

**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 switch might fail.

Configuring the Ethernet Management Port

To specify the Ethernet management port in the CLI, enter **fastethernet0**.

To disable the port, use the **shutdown** interface configuration command. To enable the port, use the **no shutdown** interface configuration command.

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.

To display the link status, use the **show interfaces fastethernet 0** privileged EXEC command.

TFTP and the Ethernet Management Port

Use the commands in [Table 13-3](#) when using TFTP to download or upload a configuration file to the boot loader.

Table 13-3 Boot Loader Commands

Command	Description
arp <i>[ip_address]</i>	Displays the currently cached ARP ¹ table when this command is entered without the <i>ip_address</i> parameter. Enables ARP to associate a MAC address with the specified IP address when this command is entered with the <i>ip_address</i> parameter.
mgmt_clr	Clears the statistics for the Ethernet management port.
mgmt_init	Starts the Ethernet management port.
mgmt_show	Displays the statistics for the Ethernet management port.
ping <i>host_ip_address</i>	Sends ICMP ECHO_REQUEST packets to the specified network host.

Table 13-3 *Boot Loader Commands (continued)*

Command	Description
<code>boot tftp:/file-url ...</code>	Loads and boots an executable image from the TFTP server and enters the command-line interface. For more details, see the command reference for this release.
<code>copy tftp:/source-file-url filesystem:/destination-file- url</code>	Copies a Cisco IOS image from the TFTP server to the specified location. For more details, see the command reference for this release.

1. ARP = Address Resolution Protocol.

Configuring Ethernet Interfaces

- [Default Ethernet Interface Configuration, page 13-27](#)
- [Setting the Type of a Dual-Purpose Uplink Port, page 13-28](#)
- [Configuring Interface Speed and Duplex Mode, page 13-30](#)
- [Configuring IEEE 802.3x Flow Control, page 13-32](#)
- [Configuring Auto-MDIX on an Interface, page 13-33](#)
- [Configuring a Power Management Mode on a PoE Port, page 13-34](#)
- [Budgeting Power for Devices Connected to a PoE Port, page 13-35](#)
- [Configuring Power Policing, page 13-37](#)
- [Configuring Catalyst PoE and PoE Pass-Through Ports on Compact Switches, page 13-39](#)
- [Adding a Description for an Interface, page 13-41](#)

Default Ethernet Interface Configuration

Table 13-4 shows the Ethernet interface default configuration. For more details on the VLAN parameters listed in the table, see [Chapter 14, “Configuring VLANs.”](#) For details on controlling traffic to the port, see [Chapter 24, “Configuring Port-Based Traffic Control.”](#)

Table 13-4 *Default Layer 2 Ethernet Interface Configuration*

Feature	Default Setting
Allowed VLAN range	VLANs 1 to 4094.
Default VLAN (for access ports)	VLAN 1.
Native VLAN (for IEEE 802.1Q trunks)	VLAN 1.
802.1p priority-tagged traffic	Drop all packets tagged with VLAN 0.
VLAN trunking	Switchport mode dynamic auto (supports DTP).
Port enable state	All ports are enabled.
Port description	None defined.

Table 13-4 Default Layer 2 Ethernet Interface Configuration (continued)

Feature	Default Setting
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. Chapter 39, “Configuring EtherChannels and Link-State Tracking.”
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked). See the “Configuring Port Blocking” section on page 24-7.
Broadcast, multicast, and unicast storm control	Disabled. See the “Default Storm Control Configuration” section on page 24-3.
Protected port	Disabled. See the “Configuring Protected Ports” section on page 24-6.
Port security	Disabled. See the “Default Port Security Configuration” section on page 24-11.
Port Fast	Disabled. See the “Default Optional Spanning-Tree Configuration” section on page 19-12.
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-MIDX is enabled on the switch port.
Power over Ethernet (PoE)	Enabled (auto).
Keepalive messages	Disabled on SFP module ports; enabled on all other ports.

Setting the Type of a Dual-Purpose Uplink Port



Note

Only Catalyst 2960 switches have dual-purpose uplinks ports.

Some switches support dual-purpose uplink ports. By default, the switch dynamically selects the interface type that first links up. However, you can use the **media-type** interface configuration command to manually select the RJ-45 connector or the SFP module connector. For more information, see the [“Dual-Purpose Uplink Ports” section on page 13-4.](#)

Beginning in privileged EXEC mode, follow these steps to select which dual-purpose uplink to activate so that you can set the speed and duplex. This procedure is optional.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the dual-purpose uplink port to be configured, and enter interface configuration mode.
Step 3	media-type { auto-select rj45 sfp }	Select the interface and type of a dual-purpose uplink port. The keywords have these meanings: <ul style="list-style-type: none"> • auto-select—The switch dynamically selects the type. When link up is achieved, the switch disables the other type until the active link goes down. When the active link goes down, the switch enables both types until one of them links up. In auto-select mode, the switch configures both types with autonegotiation of speed and duplex (the default). Depending on the type of installed SFP module, the switch might not be able to dynamically select it. For more information, see the information that follows this procedure. • rj45—The switch disables the SFP module interface. If you connect an SFP module to this port, it cannot attain a link even if the RJ-45 side is down or is not connected. In this mode, the dual-purpose port behaves like a 10/100/1000BASE-TX interface. You can configure the speed and duplex settings consistent with this interface type. • sfp—The switch disables the RJ-45 interface. If you connect a cable to the RJ-45 port, it cannot attain a link even if the SFP module side is down or if the SFP module is not present. Based on the type of installed SFP module, you can configure the speed and duplex settings consistent with this interface type. For information about setting the speed and duplex, see the “Speed and Duplex Configuration Guidelines” section on page 13-30.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> transceiver properties	Verify your setting.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **media-type auto interface** or the **no media-type** interface configuration commands.

The switch configures both types to autonegotiate speed and duplex (the default). If you configure **auto-select**, you cannot configure the **speed** and **duplex** interface configuration commands.

When the switch powers on or when you enable a dual-purpose uplink port through the **shutdown** and the **no shutdown** interface configuration commands, the switch gives preference to the SFP module interface. In all other situations, the switch selects the active link based on which type first links up.

The switch operates with 100BASE-x (where -x is -BX, -FX-FE, -LX) SFP modules as follows:

- When the 100BASE-*x* SFP module is inserted into the module slot and there is no link on the RJ-45 side, the switch disables the RJ-45 interface and selects the SFP module interface. This is the behavior even if there is no cable connected and if there is no link on the SFP module side.
- When the 100BASE-*x* SFP module is inserted and there is a link on the RJ-45 side, the switch continues with that link. If the link goes down, the switch disables the RJ-45 side and selects the SFP module interface.
- When the 100BASE-*x* SFP module is removed, the switch again dynamically selects the type (**auto-select**) and re-enables the RJ-45 side.

The switch does not have this behavior with 100BASE-FX-GE SFP modules.

Configuring Interface Speed and Duplex Mode

Depending on the supported port types, Ethernet interfaces on the switch operate at 10, 100, or 1000 Mb/s, or 10,000 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 models can include combinations of Fast Ethernet (10/100-Mb/s) ports, Gigabit Ethernet (10/100/1000-Mb/s) ports, 10-Gigabit module ports, and small form-factor pluggable (SFP) module slots supporting SFP modules.

These sections describe how to configure the interface speed and duplex mode:

- [Speed and Duplex Configuration Guidelines, page 13-30](#)
- [Setting the Interface Speed and Duplex Parameters, page 13-31](#)

Speed and Duplex Configuration Guidelines

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

- Fast Ethernet (10/100-Mb/s) ports support all speed and duplex options.
- 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.
 - The 100BASE-*x* (where *x* is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support only 100 Mb/s. These modules support full- and half- duplex options but do not support autonegotiation.

For information about which SFP modules are supported on your switch, see the product release notes.

- 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 switch can take up to 30 seconds to check for loops. The port LED is amber while STP reconfigures.

**Caution**

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

Setting the Interface Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex mode for a physical interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the physical interface to be configured, and enter interface configuration mode.
Step 3	speed { 10 100 1000 auto [10 100 1000] nonegotiate }	Enter the appropriate speed parameter for the interface: <ul style="list-style-type: none"> • Enter 10, 100, or 1000 to set a specific speed for the interface. The 1000 keyword is available only for 10/100/1000 Mb/s ports. • Enter auto to enable the interface to autonegotiate speed with the connected device. If you use the 10, 100, or the 1000 keywords with the auto keyword, the port autonegotiates only at the specified speeds. • The nonegotiate keyword is available only for SFP module ports. SFP module ports operate only at 1000 Mb/s but can be configured to not negotiate if connected to a device that does not support autonegotiation. For more information about speed settings, see the “Speed and Duplex Configuration Guidelines” section on page 13-30 .
Step 4	duplex { auto full half }	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. For more information about duplex settings, see the “Speed and Duplex Configuration Guidelines” section on page 13-30 .
Step 5	end	Return to privileged EXEC mode.
Step 6	show interfaces <i>interface-id</i>	Display the interface speed and duplex mode configuration.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no speed** and **no duplex** interface configuration commands to return the interface to the default speed and duplex settings (autonegotiate). To return all interface settings to the defaults, use the **default interface** *interface-id* interface configuration command.

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

```
Switch# configure terminal
Switch(config)# interface fasttetherenet1/0/3
Switch(config-if)# speed 10
Switch(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:

```
Switch# configure terminal
Switch(config)# interface gigabitetherenet1/0/2
Switch(config-if)# speed 100
```

Configuring 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

Ports on the switch 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**. The default state is **off**.

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.

Beginning in privileged EXEC mode, follow these steps to configure flow control on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the physical interface to be configured, and enter interface configuration mode.
Step 3	flowcontrol { receive } { on off desired }	Configure the flow control mode for the port.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i>	Verify the interface flow control settings.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable flow control, use the **flowcontrol receive off** interface configuration command.

This example shows how to turn on flow control on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)# end
```

Configuring 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 switches 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 switches 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.

Auto-MDIX is enabled by default.

Auto-MDIX is supported on all 10/100 and 10/100/1000-Mb/s interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

Table 13-5 shows the link states that result from auto-MDIX settings and correct and incorrect cabling.

Table 13-5 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

Beginning in privileged EXEC mode, follow these steps to configure auto-MDIX on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the physical interface to be configured, and enter interface configuration mode.
Step 3	speed auto	Configure the interface to autonegotiate speed with the connected device.
Step 4	duplex auto	Configure the interface to autonegotiate duplex mode with the connected device.
Step 5	end	Return to privileged EXEC mode.
Step 6	show controllers ethernet-controller <i>interface-id</i> phy	Verify the operational state of the auto-MDIX feature on the interface.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable auto-MDIX, use the **no mdix auto** interface configuration command.

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

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

Configuring a Power Management Mode on a PoE Port



Note

PoE commands are supported only when the switch is running the LAN base image. Power over Ethernet Plus (PoE+) is supported only on Catalyst 2960-S switches.

For most situations, the default configuration (auto mode) works well, providing plug-and-play operation. No further configuration is required. However, use the following procedure to give a PoE port higher priority, to make it data only, or to specify a maximum wattage to disallow high-power powered devices on a 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 switch 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 switch removes power from the port and then redetects the powered device. The switch repowers the port only if the powered device is a Class 1, Class 2, or a Cisco-only powered device.

Beginning in privileged EXEC mode, follow these steps to configure a power management mode on a PoE-capable port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the physical port to be configured, and enter interface configuration mode.

	Command	Purpose
Step 3	power inline { auto [max <i>max-wattage</i>] never static [max <i>max-wattage</i>] }	<p>Configure the PoE mode on the port. The keywords have these meanings:</p> <ul style="list-style-type: none"> • auto—Enable powered-device detection. If enough power is available, automatically allocate power to the PoE port after device detection. This is the default setting. • (Optional) max <i>max-wattage</i>—Limit the power allowed on the port. The range is 4000 to 15400 milliwatts on a PoE port and 4000 to 30000 milliwatts on a PoE+ port. If no value is specified, the maximum is allowed. • never—Disable device detection, and disable power to the port. <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 an error-disabled state.</p> <ul style="list-style-type: none"> • static—Enable powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers the powered device. The switch reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection. <p>The switch allocates power to a port configured in static mode before it allocates power to a port configured in auto mode.</p>
Step 4	end	Return to privileged EXEC mode.
Step 5	show power inline [<i>interface-id</i> <i>module switch-number</i>]	Display PoE status for a switch or switch stack, for the specified interface, or for a specified stack member. The module keyword is applicable only on Catalyst 2960-S switches running the LAN base image.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

For information about the output of the **show power inline** user EXEC command, see the command reference for this release. For more information about PoE-related commands, see the “[Troubleshooting Power over Ethernet Switch Ports](#)” section on page 40-13. For information about configuring voice VLAN, see [Chapter 16, “Configuring Voice VLAN.”](#)

Budgeting Power for Devices Connected to a PoE Port

When Cisco powered devices are connected to PoE ports, the switch uses Cisco Discovery Protocol (CDP) to determine the *actual* power consumption of the devices, and the switch adjusts the power budget accordingly. The CDP protocol works with Cisco powered devices and does not apply to IEEE third-party powered devices. For these devices, when the switch grants a power request, the switch adjusts the power budget according to the powered-device IEEE classification. If the powered device is a Class 0 (class status unknown) or a Class 3, the switch budgets 15,400 milliwatts for the device, regardless of the actual amount of power needed. If the powered device reports a higher class than its actual consumption or does not support power classification (defaults to Class 0), the switch can power fewer devices because it uses the IEEE class information to track the global power budget.

By using the **power inline consumption** *wattage* configuration command, you can override the default power requirement specified by the IEEE classification. The difference between what is mandated by the IEEE classification and what is actually needed by the device is reclaimed into the global power budget for use by additional devices. You can then extend the switch power budget and use it more effectively.

For example, if the switch budgets 15,400 milliwatts on each PoE port, you can connect only 24 Class 0 powered devices. If your Class 0 device power requirement is actually 5000 milliwatts, you can set the consumption wattage to 5000 milliwatts and connect up to 48 devices. The total PoE output power available on a 24-port or 48-port switch is 370,000 milliwatts.

**Caution**

You should carefully plan your switch power budget and make certain not to oversubscribe the power supply.

**Note**

When you manually configure the power budget, you must also consider the power loss over the cable between the switch and the powered device.

When you enter the **power inline consumption default** *wattage* or the **no power inline consumption default** global configuration command, or the **power inline consumption** *wattage* or the **no power inline consumption** interface configuration command this caution message appears:

```
%CAUTION: Interface interface-id: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty. Take precaution not to
oversubscribe the power supply.
```

```
It is recommended to enable power policing if the switch supports it.
Refer to documentation.
```

If the power supply is over-subscribed to by up to 20 percent, the switch continues to operate but its reliability is reduced. If the power supply is subscribed to by more than 20 percent, the short-circuit protection circuitry triggers and shuts the switch down.

For more information about the IEEE power classifications, see the [“Power over Ethernet Ports” section on page 13-5](#).

Beginning in privileged EXEC mode, follow these steps to configure the amount of power budgeted to a powered device connected to each PoE port on a switch:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	no cdp run	(Optional) Disable CDP.
Step 3	power inline consumption default <i>wattage</i>	Configure the power consumption of powered devices connected to each the PoE port on the switch. The range for each device is 4000 to 15400 milliwatts on a PoE switch and 4000 to 30000 milliwatts on a PoE+ switch. The default is 15400 milliwatts on a PoE switch and 30000 milliwatts on a PoE+ switch. Note When you use this command, we recommend you also enable power policing.
Step 4	end	Return to privileged EXEC mode.
Step 5	show power inline consumption	Display the power consumption status.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no power inline consumption default** global configuration command.

Beginning in privileged EXEC mode, follow these steps to configure amount of power budgeted to a powered device connected to a specific PoE port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	no cdp run	(Optional) Disable CDP.
Step 3	interface <i>interface-id</i>	Specify the physical port to be configured, and enter interface configuration mode.
Step 4	power inline consumption <i>wattage</i>	Configure the power consumption of a powered device connected to a PoE port on the switch. The range for each device is 4000 to 15400 milliwatts on a PoE port and 4000 to 30000 milliwatts on a PoE+ port. The default is 15400 milliwatts on a PoE port and 30000 milliwatts on a PoE+ port. Note When you use this command, we recommend you also enable power policing.
Step 5	end	Return to privileged EXEC mode.
Step 6	show power inline consumption	Display the power consumption status.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no power inline consumption** interface configuration command.

For information about the output of the **show power inline consumption** privileged EXEC command, see the command reference for this release.

Configuring Power Policing

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

For more information about the cutoff power value, the power consumption values that the switch uses, and the actual power consumption value of the connected device, see the “Power Monitoring and Power Policing” section.

Beginning in privileged EXEC mode, follow these steps to enable policing of the real-time power consumption of a powered device connected to a PoE port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the physical port to be configured, and enter interface configuration mode.

	Command	Purpose
Step 3	power inline police [action {errdisable log}]	<p>If the real-time power consumption exceeds the maximum power allocation on the port, configure the switch to take one of these actions:</p> <ul style="list-style-type: none"> Shut down the PoE port, turn off power to it, and put it in the error-disabled state—Enter the power inline police command. <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 interval global configuration command.</p> <ul style="list-style-type: none"> Generate a syslog message while still providing power to the port—Enter the power inline police action log command. <p>If you do not enter the action keywords, the default action shuts down the port and puts the port in the error-disabled state.</p>
Step 4	exit	Return to global configuration mode.
Step 5	errdisable detect cause inline-power and errdisable recovery cause inline-power and errdisable recovery interval interval	<p>(Optional) Enable error recovery from the PoE error-disabled state, and configure the PoE recover mechanism variables.</p> <p>For interval interval, specify the time in seconds to recover from the error-disabled state. The range is 30 to 86400.</p> <p>By default, the recovery interval is 300 seconds.</p>
Step 6	exit	Return to privileged EXEC mode.
Step 7	show power inline police show errdisable recovery	Display the power monitoring status, and verify the error recovery settings.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable policing of the real-time power consumption, use the **no power inline police** interface configuration command. To disable error recovery for PoE error-disabled cause, use the **no errdisable recovery cause inline-power** global configuration command.

For information about the output from the **show power inline police** privileged EXEC command, see the command reference for this release.

Configuring Catalyst PoE and PoE Pass-Through Ports on Compact Switches

You can configure the power management, budgeting, and policing on the Catalyst 2960-C compact switch PoE ports the same as with any other PoE switch.

The **show env power inline** privileged EXEC command provides information about powering options and power backup on your switch:

```
Switch# show env power
PoE Power - Available:22.4(w) Backup:0.0(w)

Power Source   Type           Power(w)  Mode
-----
A.C. Input     Auxilliary     51(w)     Available
Gi0/2          Type1          15.4(w)   Back-up
```

Available : The PoE received on this link is used for powering this switch and providing PoE pass-through if applicable.

Back-up : In the absence of 'Available' power mode, the PoE received on this link is used for powering this switch and providing PoE pass-through if applicable.

Available* : The PoE received on this link is used for powering this switch but does not contribute to the PoE pass-through.

Back-up* : In the absence of 'Available' power mode, the PoE received on this link is used for powering this switch but does not contribute to the PoE pass-through.

You can see the available power and the power required by each connected device by entering the **show power inline** privileged EXEC command.

This is an example of output from a Catalyst 2960CPD-8PT, capable of providing pass-through power:

```
Switch# show power inline
Available:22.4(w) Used:15.4(w) Remaining:7.0(w)

Interface Admin Oper      Power Device           Class Max
          (Watts)
-----
Fa0/1     auto  off      0.0   n/a                 n/a  15.4
Fa0/2     auto  off      0.0   n/a                 n/a  15.4
Fa0/3     auto  off      0.0   n/a                 n/a  15.4
Fa0/4     auto  off      0.0   n/a                 n/a  15.4
Fa0/5     auto  on       15.4  IP Phone 8961       4    15.4
Fa0/6     auto  off      0.0   n/a                 n/a  15.4
Fa0/7     auto  off      0.0   n/a                 n/a  15.4
Fa0/8     auto  off      0.0   n/a                 n/a  15.4
```

Enter the **show power inline police** privileged EXEC command to see power monitoring status.

This is an example of output from a Catalyst 2960CPD-8PT:

```
Switch# show power inline police
Available:22.4(w)  Used:15.4(w)  Remaining:7.0(w)
```

Interface	Admin State	Oper State	Admin Police	Oper Police	Cutoff Power	Oper Power
Fa0/1	auto	off	none	n/a	n/a	0.0
Fa0/2	auto	off	none	n/a	n/a	0.0
Fa0/3	auto	off	none	n/a	n/a	0.0
Fa0/4	auto	off	none	n/a	n/a	0.0
Fa0/5	auto	on	none	n/a	n/a	9.5
Fa0/6	auto	off	none	n/a	n/a	0.0
Fa0/7	auto	off	none	n/a	n/a	0.0
Fa0/8	auto	off	none	n/a	n/a	0.0
Totals:						9.5

The Catalyst 2960CPD-8TT and Catalyst 2960CG-8TC downlink ports cannot provide power to end devices. This is an example of output from the **show power inline** command on a C2960CPD-8TT switch:

```
Switch# show power inline
Available:0.0(w)  Used:0.0(w)  Remaining:0.0(w)
```

Interface	Admin	Oper	Power (Watts)	Device	Class	Max

The **show power inline dynamic-priority** command shows the power priority of each port:

```
Switch# show power inline dynamic-priority
Dynamic Port Priority
-----
```

Port	OperState	Priority
Fa0/1	off	High
Fa0/2	off	High
Fa0/3	off	High
Fa0/4	off	High
Fa0/5	off	High
Fa0/6	off	High
Fa0/7	off	High
Fa0/8	off	High

Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description appears in the output of these privileged EXEC commands: **show configuration**, **show running-config**, and **show interfaces**.

Beginning in privileged EXEC mode, follow these steps to add a description for an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the interface for which you are adding a description, and enter interface configuration mode.
Step 3	description <i>string</i>	Add a description (up to 240 characters) for an interface.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> description or show running-config	Verify your entry.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no description** interface configuration command to delete the description.

This example shows how to add a description on a port and how to verify the description:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/0/2 description
Interface Status      .Protocol Description
Gi1/0/2    admin down      down      Connects to Marketing
```

Configuring Layer 3 SVIs



Note

Only switches running the LAN base image support Layer 3 SVIs for static routing.

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 VLAN 1.



Note

When you create an SVI, it does not become active until you associate it with a physical port. For information about assigning Layer 2 ports to VLANs, see [Chapter 14, “Configuring VLANs.”](#)

A Layer 3 switch can have an IP address assigned to each SVI, but the switch supports static routing on 16 SVIs. 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.

Beginning in privileged EXEC mode, follow these steps to configure a Layer 3 SVI:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface vlan <i>vlan-id</i>	Specify the VLAN to be configured as a Layer 3 SVI, and enter interface configuration mode.
Step 3	ip address <i>ip_address subnet_mask</i>	Configure the IP address and IP subnet.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interfaces [<i>interface-id</i>] show ip interface [<i>interface-id</i>] show running-config interface [<i>interface-id</i>]	Verify the configuration.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove an IP address from an SVI, use the **no ip address** interface configuration command.

This example shows how to configure a Layer 3 SVI and to assign it an IP address:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 33
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
```

Configuring the System MTU

The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces is 1500 bytes. You can increase the MTU size for all interfaces operating at 10 or 100 Mb/s by using the **system mtu** global configuration command. You can increase the MTU size to support jumbo frames on all Gigabit Ethernet interfaces by using the **system mtu jumbo** global configuration command.

Gigabit Ethernet ports are not affected by the **system mtu** command; 10/100 ports are not affected by the **system mtu jumbo** command. If you do not configure the **system mtu jumbo** command, the setting of the **system mtu** command applies to all Gigabit Ethernet interfaces.

You cannot set the MTU size for an individual interface; you set it for all 10/100 or all Gigabit Ethernet interfaces. When you change the system or jumbo MTU size, you must reset the switch before the new configuration takes effect.

Frames sizes that can be received by the switch CPU are limited to 1998 bytes, no matter what value was entered with the **system mtu** or **system mtu jumbo** commands. Although frames that are forwarded are typically not received by the CPU, in some cases, packets are sent to the CPU, such as traffic sent to control traffic, SNMP, or Telnet.

**Note**

If Layer 2 Gigabit Ethernet interfaces are configured to accept frames greater than the 10/100 interfaces, jumbo frames received on a Layer 2 Gigabit Ethernet interface and sent on a Layer 2 10/100 interface are dropped.

Beginning in privileged EXEC mode, follow these steps to change MTU size for all 10/100 or Gigabit Ethernet interfaces:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	system mtu bytes	(Optional) Change the MTU size for all interfaces on the switch stack that are operating at 10 or 100 Mb/s. The range is 1500 to 1998 bytes; the default is 1500 bytes.
Step 3	system mtu jumbo bytes	(Optional) Change the MTU size for all Gigabit Ethernet interfaces on the switch. (Optional) Change the MTU size for all Gigabit Ethernet interfaces on the switch stack. The range is 1500 to 9198 bytes; the default is 1500 bytes.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	Save your entries in the configuration file.
Step 6	reload	Reload the operating system.

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

Once the switch reloads, you can verify your settings by entering the **show system mtu** privileged EXEC command.

This example shows how to set the maximum packet size for a Gigabit Ethernet port to 1800 bytes:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

This example shows the response when you try to set Gigabit Ethernet interfaces to an out-of-range number:

```
Switch(config)# system mtu jumbo 25000
                        ^
% Invalid input detected at '^' marker.
```

Monitoring and Maintaining the Interfaces

These sections contain interface monitoring and maintenance information:

- [Monitoring Interface Status, page 13-44](#)
- [Clearing and Resetting Interfaces and Counters, page 13-45](#)
- [Shutting Down and Restarting the Interface, page 13-45](#)

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 13-6](#) lists some of these interface monitoring commands. (You can display the full list of **show** commands by using the **show ?** command at the privileged EXEC prompt.) These commands are fully described in the *Cisco IOS Interface Command Reference, Release 12.4* from Cisco.com.

Table 13-6 Show Commands for Interfaces

Command	Purpose
show interfaces [<i>interface-id</i>]	(Optional) Display the status and configuration of all interfaces or a specific interface.
show interfaces <i>interface-id</i> status [err-disabled]	(Optional) Display interface status or a list of interfaces in an error-disabled state.
show interfaces [<i>interface-id</i>] switchport	(Optional) Display administrative and operational status of switching ports.
show interfaces [<i>interface-id</i>] description	(Optional) Display the description configured on an interface or all interfaces and the interface status.
show ip interface [<i>interface-id</i>]	(Optional) Display the usability status of all interfaces configured for IP routing or the specified interface.
show interface [<i>interface-id</i>] stats	(Optional) Display the input and output packets by the switching path for the interface.
show interfaces transceiver properties	(Optional) Display speed and duplex settings on the interface.
show interfaces [<i>interface-id</i>] [{ transceiver properties detail }] [<i>module number</i>]	Display physical and operational status about an SFP module.
show running-config interface [<i>interface-id</i>]	Display the running configuration in RAM for the interface.
show version	Display 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	Display the operational state of the auto-MDIX feature on the interface.
show power inline [<i>interface-id</i>]	Display PoE status for a switch or for an interface.
show power inline police	Display the power policing data.

Clearing and Resetting Interfaces and Counters

Table 13-7 lists the privileged EXEC mode **clear** commands that you can use to clear counters and reset interfaces.

Table 13-7 Clear Commands for Interfaces

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

To clear the interface counters shown by the **show interfaces** privileged EXEC command, use the **clear counters** privileged EXEC command. The **clear counters** command clears all current interface counters from the interface unless you specify optional arguments that clear only a specific interface type from a specific interface number.



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.

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.

Beginning in privileged EXEC mode, follow these steps to shut down an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface { <i>vlan vlan-id</i> } {{ <i>fastethernet</i> <i>gigabitethernet</i> } <i>interface-id</i> } { <i>port-channel port-channel-number</i> }	Select the interface to be configured.
Step 3	shutdown	Shut down an interface.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entry.

