



CHAPTER 1

Configuring Interface Characteristics

This chapter defines the types of interfaces on the Catalyst 3750-X or 3560-X switch and describes how to configure them. Unless otherwise noted, the term *switch* refers to a Catalyst 3750-X or 3560-X standalone switch and to a Catalyst 3750-X switch stack.

The chapter consists of these sections:

- [Interface Types, page 1-1](#)
- [Using the Switch USB Ports, page 1-16](#)
- [Using Interface Configuration Mode, page 1-20](#)
- [Using the Ethernet Management Port, page 1-26](#)
- [Configuring Ethernet Interfaces, page 1-30](#)
- [Configuring Layer 3 Interfaces, page 1-40](#)
- [Configuring the System MTU, page 1-43](#)
- [Configuring the Power Supplies, page 1-46](#)
- [Configuring the Cisco RPS 2300 in a Mixed Stack, page 1-46](#)
- [Configuring the Cisco eXpandable Power System \(XPS\) 2200, page 1-48](#)
- [Monitoring and Maintaining the Interfaces, page 1-51](#)



Note

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

Interface Types

This section describes the different types of interfaces supported by the switch with references to chapters that contain more detailed information about configuring these interface types. The rest of the chapter describes configuration procedures for physical interface characteristics.



Note

The stack ports on the rear of the Catalyst 3750-X switch are not Ethernet ports and cannot be configured.

These sections describe the interface types:

- [Port-Based VLANs, page 1-2](#)
- [Switch Ports, page 1-3](#)
- [Routed Ports, page 1-4](#)
- [Switch Virtual Interfaces, page 1-5](#)
- [EtherChannel Port Groups, page 1-6](#)
- [10-Gigabit Ethernet Interfaces, page 1-7](#)
- [Power over Ethernet Ports, page 1-7](#)
- [Universal Power Over Ethernet, page 1-13](#)
- [Network Module Interfaces, page 1-14](#)
- [Connecting Interfaces, page 1-15](#)

Port-Based VLANs

A VLAN is a switched network that is logically segmented by function, team, or application, without regard to the physical location of the users. For more information about VLANs, see [Chapter 1, “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 a local port is configured to be associated with the VLAN, when the VLAN Trunking Protocol (VTP) learns of its existence from a neighbor on a trunk, or when a user creates a VLAN. VLANs can be formed with ports across the stack.

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

In a switch 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.

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.
- For a tunnel port, set and define the VLAN ID for the customer-specific VLAN tag. See [Chapter 1, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”](#)

Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. Switch ports belong to one or more VLANs. A switch port can be an access port, a trunk port, or a tunnel 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. You must manually configure tunnel ports as part of an asymmetric link connected to an IEEE 802.1Q trunk port. Switch ports are used for managing the physical interface and associated Layer 2 protocols and do not handle routing or bridging.

Configure switch ports by using the **switchport** interface configuration commands. Use the **switchport** command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode.

**Note**

When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

For detailed information about configuring access port and trunk port characteristics, see [Chapter 1, “Configuring VLANs.”](#) For more information about tunnel ports, see [Chapter 1, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”](#)

Access Ports

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

Two types of access ports are supported:

- 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 Readiness Check”](#) section on page 1-15.)
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is not a member of any VLAN, and forwarding to and from the port is enabled only when the VLAN membership of the port 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 3750-X or 3560-X 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 1, “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. These trunk port types are supported:

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

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

For more information about trunk ports, see [Chapter 1, “Configuring VLANs.”](#)

Tunnel Ports

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

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

For more information about tunnel ports, see [Chapter 1, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”](#)

Routed Ports

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

**Note**

Routed ports are not supported on switches running the LAN Base feature set. However, starting with Cisco IOS release 12.2(58)SE, you can configure up to 16 static routes on SVIs.

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

**Note**

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

The number of routed ports that you can configure is not limited by software. However, the interrelationship between this number and the number of other features being configured might impact CPU performance because of hardware limitations. See the “[Configuring Layer 3 Interfaces](#)” section on page 1-40 for information about what happens when hardware resource limitations are reached.

For more information about IP unicast and multicast routing and routing protocols, see [Chapter 1, “Configuring IP Unicast Routing”](#) and [Chapter 1, “Configuring IP Multicast Routing.”](#)

**Note**

The IP Base feature set supports static routing and the Routing Information Protocol (RIP). Starting with Cisco IOS Release 12.2(58)E, the LAN Base feature set supports 16 user-configured static routes on SVIs. For full Layer 3 routing or for fallback bridging, you must enable the IP Services feature set on the standalone switch, or the active switch.

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. Only one SVI can be associated with a VLAN, but you need to configure an SVI for a VLAN only when you want to route between VLANs, to fallback-bridge nonroutable protocols 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; in Layer 3 mode, you can configure routing across SVIs.

Although the switch stack or switch supports a total of 1005 VLANs and SVIs (255 if the switch is running the LAN Base feature set), the interrelationship between the number of SVIs and routed ports and the number of other features being configured might impact CPU performance because of hardware limitations. See the “[Configuring Layer 3 Interfaces](#)” section on page 1-40 for information about what happens when hardware resource limitations are reached.

SVIs are created the first time that you enter the **vlan** interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an ISL or IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address. For more information, see the [“Manually Assigning IP Information” section on page 1-15](#).

**Note**

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

SVIs support routing protocols and bridging configurations. For more information about configuring IP routing, see [Chapter 1, “Configuring IP Unicast Routing,”](#) [Chapter 1, “Configuring IP Multicast Routing,”](#) and [Chapter 1, “Configuring Fallback Bridging.”](#)

**Note**

The LAN Base feature set supports only static routing on SVIs. The IP Base feature set supports static routing and RIP. For more advanced routing or for fallback bridging, enable the IP Services feature set on the standalone switch or the active switch. For information about using the software activation feature to install a software license for a specific feature set, see the *Cisco IOS Software Activation* document.

SVI Autostate Exclude

The line state of an SVI with multiple ports on a VLAN is in the *up* state when it meets these conditions:

- The VLAN exists and is active in the VLAN database on the switch.
- The VLAN interface exists and is not administratively down.
- At least one Layer 2 (access or trunk) port exists, has a link in the *up* state on this VLAN, and is in the spanning-tree forwarding state on the VLAN.

**Note**

The protocol link state for VLAN interfaces comes up when the first switch port belonging to the corresponding VLAN link comes up and is in STP forwarding state.

The default action, when a VLAN has multiple ports, is that the SVI goes down when all ports in the VLAN go down. You can use the SVI autostate exclude feature to configure a port so that it is not included in the SVI line-state up-an- down calculation. For example, if the only active port on the VLAN is a monitoring port, you might configure autostate exclude on that port so that the VLAN goes down when all other ports go down. When enabled on a port, **autostate exclude** applies to all VLANs that are enabled on that port.

The VLAN interface is brought up when one Layer 2 port in the VLAN has had time to converge (transition from STP listening-learning state to forwarding state). This prevents features such as routing protocols from using the VLAN interface as if it were fully operational and minimizes other problems, such as routing black holes. For information about configuring autostate exclude, see the [“Configuring SVI Autostate Exclude” section on page 1-42](#).

EtherChannel Port Groups

EtherChannel port groups consider multiple switch ports to be one switch port. These port groups act 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, group multiple access ports into one logical access port, group multiple tunnel ports into one logical tunnel port, or group multiple routed ports into one logical routed port. Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. Exceptions are the DTP, the Cisco Discovery Protocol (CDP), and the Port Aggregation Protocol (PAgP), which operate only on physical ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel. For Layer 3 interfaces, you manually create the logical interface by using the **interface port-channel** global configuration command. Then you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command. For Layer 2 interfaces, use the **channel-group** interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together. For more information, see [Chapter 1, “Configuring EtherChannels and Link-State Tracking.”](#)

10-Gigabit Ethernet Interfaces

The Catalyst 3750-X and 3560-X switches have a network module slot into which you can insert a 10-Gigabit Ethernet network module, a 1-Gigabit Ethernet network module, or a blank module.

A 10-Gigabit Ethernet interface operates only in full-duplex mode. The interface can be configured as a switched or routed port.

For more information about the Cisco TwinGig Converter Module, see the switch hardware installation guide and your transceiver module documentation.

Power over Ethernet Ports

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

- Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- IEEE 802.3af-compliant powered device
- IEEE 802.3at-compliant powered device

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

After the switch detects a powered device, the switch 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 1-8](#)
- [Powered-Device Detection and Initial Power Allocation, page 1-8](#)
- [Power Management Modes, page 1-10](#)
- [Power Monitoring and Power Policing, page 1-11](#)

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-upon 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—The PoE+ standard increases the maximum power that can be drawn by a powered device from 15.4 W per port to 30 W per port. The 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 1-13](#).

Powered-Device Detection and Initial Power Allocation

The switch detects a Cisco prestandard 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 adapter.

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 the switch allocates 15.4 W as the initial allocation for power budgeting.

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 1-1](#) lists these levels.

Table 1-1 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 (For IEEE 802.3at Type 2 powered devices)

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 *CDP-specific* power consumption requirement of the connected Cisco powered devices, which is the amount of power to allocate based on the CDP messages. The 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.

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

**Note**

The initial allocation for Class 0, Class 3, and Class 4 powered devices is 15.4 W. When a device starts up and uses CDP or LLDP to send a request for more than 15.4 W, it can be allocated up to the maximum of 30 W.

**Note**

The CDP-specific power consumption requirement is referred to as the *actual* power consumption requirement in the Catalyst 3750 and 3560 software configuration guides and command references.

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.

The Catalyst 3750-X stackable switch also supports StackPower, which allows the power supplies to share the load across multiple systems in a stack when you connect the switches with power stack cables. You can manage the power supplies of up to four stack members as a one large power supply. For more information about StackPower, see [Chapter 1, “Configuring Catalyst 3750-X StackPower.”](#)

Power Management Modes

The switch supports these 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 switch shuts down the powered device.

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 that 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 1-35.

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

Power monitoring is backward-compatible with Cisco intelligent power management and CDP-based power consumption. It works with these features to ensure that the PoE port can supply power to the powered device. For more information about these PoE features, see the [“Supported Protocols and Standards” section on page 1-8](#).

The switch senses the real-time 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. The switch reports the information through the 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 1-11](#).

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 one of these values as 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 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 are 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 on 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 a standalone switch supports internal power supplies, 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 in auto mode in descending order of the port numbers. If the switch still does not have enough power, the switch then 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.

The Catalyst 3750-X stackable switch also supports StackPower, which allows power supplies to share the load across multiple systems in a stack by connecting the switches with power stack cables. You can collectively manage the power supplies of up to four stack members as a one large power supply. For more information about StackPower, see [Chapter 1, “Configuring Catalyst 3750-X StackPower.”](#)

Universal Power Over Ethernet



Note

This feature is available on switches running Cisco IOS Release 15.0(2)SE2 and higher.

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.

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
```

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.

Network Module Interfaces

The uplink ports on the 10-Gigabit service module and on the 10-Gigabit Ethernet network module are labeled *Te1/Gi2* and *Te2/Gi4*. These ports can operate at either 1 Gigabit per second or 10 Gigabits per second. They are identified in software as **gigabitethernet** *x/1/2* and *x/1/4* and **tengigabitethernet** *x/1/1* and *x/1/2*, with *x* being the switch number on Catalyst 3750-X stacks. The Catalyst 3560-X switch port numbers are the same, with no switch number.

Network Services Module

The Catalyst 3750-X and 3560-X Network Services Module (C3KX-SM-10G) uplink slots support either 1-Gigabit SFP modules or 10-Gigabit SFP+ modules. See the *Installation Notes for the Catalyst 3750-X and 3560-X Network Modules* for more details.

When you install a network services module in a Catalyst 3560-X or 3750-X switch, you can configure the 1-Gigabit and 10-Gigabit Ethernet uplink ports for the same features as any other ports in the switch. The network services module uplink ports also support Flexible NetFlow and switch-to-switch MACsec uplink encryption (link layer security).

10-Gigabit Ethernet Network Module

The C3KX-NM-10GT 10-Gigabit Ethernet Network Module has two 10-Gigabit Ethernet copper ports that can operate at either 1 Gigabit per second or 10 Gigabits per second. To configure the port speed to 1 Gigabit per second, use the **hw-module switch** global configuration command. See the command reference for command syntax description.



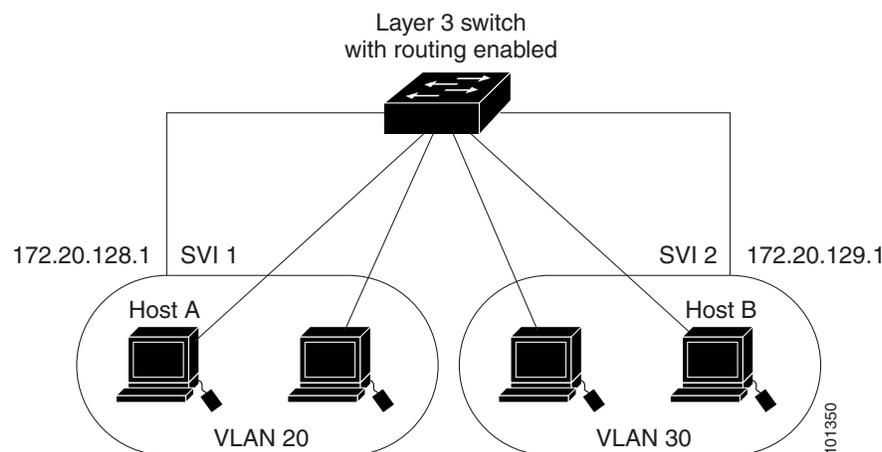
Note

10 Mb/s and 100 Mb/s speeds are not supported on this module.

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. 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 1-1).

Figure 1-1 Connecting VLANs with the 3750-X or 3560-X Switch



When the IP services feature set is running on the switch or the active switch, the switch uses two methods to forward traffic between interfaces: routing and fallback bridging. If the IP base feature set is on the switch or the active switch, only basic routing (static routing and RIP) is supported. Whenever possible, to maintain high performance, forwarding is done by the switch hardware. However, only IPv4 packets with Ethernet II encapsulation are routed in hardware. Non-IP traffic and traffic with other encapsulation methods are fallback-bridged by hardware.

- The routing function can be enabled on all SVIs and routed ports. The switch routes only IP traffic. When IP routing protocol parameters and address configuration are added to an SVI or routed port, any IP traffic received from these ports is routed. For more information, see [Chapter 1, “Configuring IP Unicast Routing,”](#) [Chapter 1, “Configuring IP Multicast Routing,”](#) and [Chapter 1, “Configuring MSDP.”](#)
- Fallback bridging forwards traffic that the switch does not route or traffic belonging to a nonroutable protocol, such as DECnet. Fallback bridging connects multiple VLANs into one bridge domain by bridging between two or more SVIs or routed ports. When configuring fallback bridging, you assign

SVIs or routed ports to bridge groups with each SVI or routed port assigned to only one bridge group. All interfaces in the same group belong to the same bridge domain. For more information, see [Chapter 1, “Configuring Fallback Bridging.”](#)

**Note**

Switches running the LAN Base feature set support configuring only 16 static routes on SVIs. Fallback bridging is not supported on the LAN Base feature set.

Using the Switch USB Ports

- [USB Mini-Type B Console Port, page 1-16](#)
- [USB Type A Port, page 1-18](#)

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. Each switch in a stack issues this log. Every switch always first displays the RJ-45 media type.

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

If you configure the RJ-45 console, USB console operation is disabled, and input always remains with the RJ-45 console. This configuration is global and applies to all switches in a stack.

To select the RJ-45 console media type, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	line console 0	Configures the console. Enter line configuration mode.
Step 3	media-type rj45	Configures 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	Returns to privileged EXEC mode.
Step 5	show running-configuration	Verifies your setting.
Step 6	copy running-config startup-config	(Optional) Saves 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 immediately terminates any active USB consoles in the stack. A log shows that this termination has occurred. This sample log 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 if the USB console is activated but no input activity occurs on it for a specified time period. When the USB console 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.

To configure an inactivity timeout, follow these steps beginning in privileged EXEC mode:

	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 no timeout.
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 for the configured number of minutes, the console reverts to RJ-45, 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 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 Cisco 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.

Booting from the USB Flash Device

To allow booting from the USB flash device, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	boot system flash usbflash0: <i>image</i>	Configures 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	Verifies your setting.
Step 4	copy running-config startup-config	(Optional) Saves 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 3750-X flash device. The image is the Catalyst 3750-X universal image.

```
Switch# configure terminal
Switch(config)# boot system flash usbflash0: c3750x-universal-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 and routed 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 1-22).

To configure a physical interface (port), specify the interface type, stack member number (only Catalyst 3750-X switches), module number, and switch port number, and enter interface configuration mode.

- Type—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 (gigabitethernet or gi).
- Stack member number—The number that identifies the switch within the stack. The switch number range is 1 to 9 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.

For information about stack member numbers, see the [“Stack Member Numbers”](#) section on page 1-7.

- Module number—The module or slot number on the switch that is always 0.
- Port number—The interface number on the switch. The 10/100/1000 port numbers always begin at 1, starting with the far left port when facing the front of the switch, for example, gigabitethernet1/0/1 or gigabitethernet1/0/8.

On a switch with 10/100/1000 ports and Cisco TwinGig Converter Modules in the 10-Gigabit Ethernet module slots, the port numbers restart with the 10-Gigabit Ethernet ports: `tengigabitethernet1/0/1`.

On a switch with 10/100/1000 ports and Cisco dual SFP X2 converter modules in the 10-Gigabit Ethernet module slots, the SFP module ports are numbered consecutively following the 10/100/1000 interfaces. For example, if the switch has 24 10/100/1000 ports, the SFP module ports are `gigabitethernet1/0/25` through `gigabitethernet1/0/28`.

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

These are examples of how to identify interfaces on a 3750-X switch:

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

```
Switch(config)# interface gigabitethernet1/0/4
```
- To configure 10-Gigabit Ethernet port 1 on a standalone switch, enter this command:

```
Switch(config)# interface tengigabitethernet1/0/1
```
- To configure 10-Gigabit Ethernet port on stack member 3, enter this command:

```
Switch(config)# interface tengigabitethernet3/0/1
```

If the switch has SFP modules, the port numbers continue consecutively. To configure the first SFP module port on stack member 1 with 16 10/100/1000 ports, enter this command:

```
Switch(config)# interface gigabitethernet1/0/25
```

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 (only on Catalyst 3750-X switches), and the number of the connector. In this example, Gigabit Ethernet port 1 on switch 1 is selected:

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



Note You do not need to add a space between the interface type and the interface number. For example, in the preceding line, you can specify either **gigabitethernet 1/0/1**, **gigabitethernet1/0/1**, **gi 1/0/1**, or **gi1/0/1**.

Step 3 Follow each **interface** command with the interface 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 1-51.

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.

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

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface range { <i>port-range</i> macro <i>macro_name</i> }	Specifies the range of interfaces (VLANs or physical ports) to be configured, and enter interface-range configuration mode. <ul style="list-style-type: none"> You can use the interface range command to configure up to five port ranges or a previously defined macro. The macro variable is explained in the “Configuring and Using Interface Range Macros” section on page 1-24. 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 reenter 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	Returns to privileged EXEC mode.
Step 5	show interfaces [<i>interface-id</i>]	Verifies the configuration of the interfaces in the range.
Step 6	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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

- Valid entries for *port-range*:
 - vlan** *vlan-ID* - *vlan-ID*, where the *VLAN ID* is 1 to 4094
 - gigabitethernet module**/*{first port}* - *{last port}* (for 3560-X switches), where the module is always 0

- **gigabitethernet stack member/module/{first port} - {last port}** (for 3750-X switches), where the module is always 0.
- **tengigabitethernet module/{first port} - {last port}** (for 3560-X switches), where the module is always 0.
- **tengigabitethernet stack member/module/{first port} - {last port}** (for 3750-X switches), where the module is always 0.
- **gigabitethernet stack member/module/{first port} - {last port}**, where the module is always 0.
- **tengigabitethernet stack member/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 48.



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, the command **interface range gigabitethernet1/0/1 - 4** is a valid range; the command **interface range gigabitethernet1/0/1-4** is not a valid range.
- 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 Gigabit Ethernet ports, all 10-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 to 100 Mb/s on ports 1 to 4 on switch 1:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 4
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 Gigabit Ethernet ports 1 to 3 and 10-Gigabit Ethernet ports 1 and 2 to receive flow-control pause frames:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 3 , tengigabitethernet1/0/1 - 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.

To define an interface range macro, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	define interface-range <i>macro_name</i> <i>interface-range</i>	Defines the interface-range macro, and saves 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.
Step 3	interface range macro <i>macro_name</i>	Selects the interface range to be configured using the values saved in the interface-range macro called <i>macro_name</i> . You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro.
Step 4	end	Returns to privileged EXEC mode.
Step 5	show running-config include define	Shows the defined interface range macro configuration.
Step 6	copy running-config startup-config	(Optional) Saves 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*:
 - vlan** *vlan-ID* - *vlan-ID*, where the *VLAN ID* is 1 to 4094
 - gigabitethernet module**/*{first port}* - *{last port}* (for 3560-X switches), where the module is always 0
 - gigabitethernet stack member/module**/*{first port}* - *{last port}* (for 3750-X switches), where the module is always 0
 - tengigabitethernet module**/*{first port}* - *{last port}* (for 3560-X switches), where the module is always 0
 - tengigabitethernet stack member/module**/*{first port}* - *{last port}* (for 3750-X switches), where the module is always 0
 - gigabitethernet stack member/module**/*{first port}* - *{last port}*, where the module is always 0
 - tengigabitethernet stack member/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 48.



Note When you use the interface ranges 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-range*. For example, **gigabitethernet1/0/1 - 4** is a valid range; **gigabitethernet1/0/1-4** is not a valid range.
- 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 Gigabit Ethernet ports, all 10-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 on switch 1 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
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,
gigabitethernet1/0/5 - 7, tengigabitethernet1/0/1 -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

This section has this information:

- [Understanding the Ethernet Management Port, page 1-26](#)
- [Supported Features on the Ethernet Management Port, page 1-28](#)
- [Configuring the Ethernet Management Port, page 1-29](#)
- [TFTP and the Ethernet Management Port, page 1-29](#)

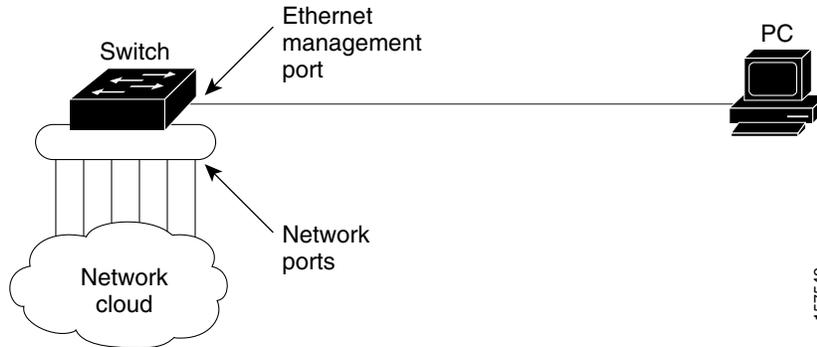
Understanding the Ethernet Management Port

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 3750-X or Catalyst 3750-E stack member.

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

For a Catalyst 3560-X switch or a standalone Catalyst 3750-X switch, connect the Ethernet management port to the PC as shown in Figure 1-2.

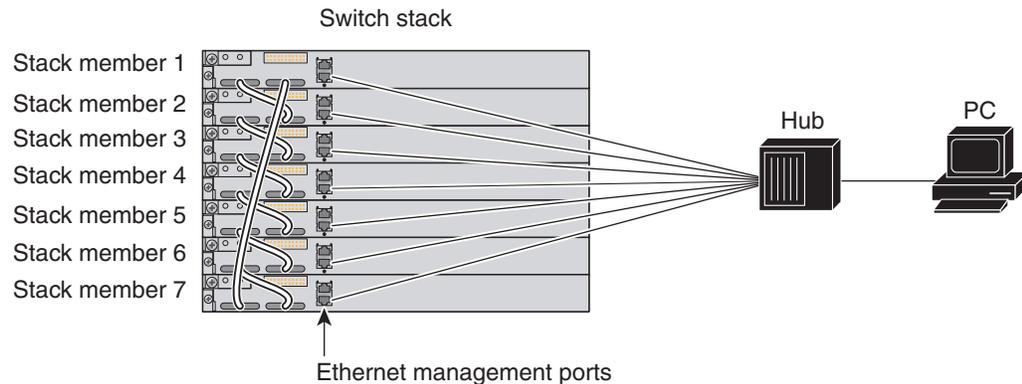
Figure 1-2 Connecting a Switch to a PC



In a stack with only Catalyst 3750-X or Catalyst 3750-E switches, all the Ethernet management ports on the stack members are connected to a hub to which the PC is connected. The active link is from the Ethernet management port on the active switch through the hub to the PC. If the active switch fails and a new active switch is elected, the active link is now from the Ethernet management port on the new active switch to the PC. See Figure 1-3.

In a mixed switch stack with Catalyst 3750 switches, only the Catalyst 3750-E and Catalyst 3750-X stack members are connected to the PC through the Ethernet management ports. The active link is from the active switch, a Catalyst 3750-E or Catalyst 3750-X switch to the PC. If the active switch fails and the elected active switch is not a Catalyst 3750-E or Catalyst 3750-X switch (switch 2), the active link can be from a stack member to the PC.

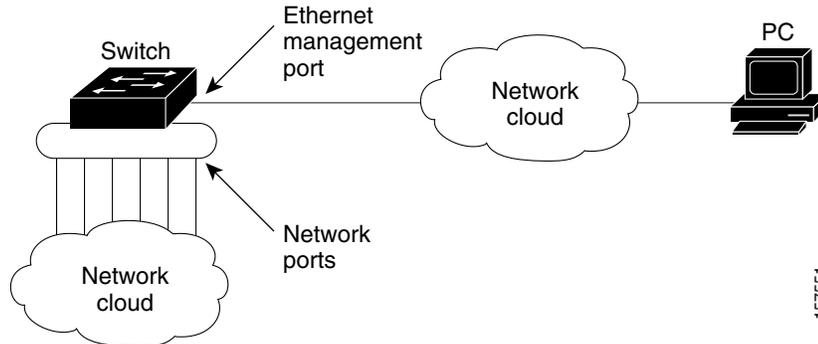
Figure 1-3 Connecting a Switch Stack to a PC



Catalyst 3750 switches do not have Ethernet management ports.
Catalyst 3750 switches in a mixed stack are not connected to the hub.

By default, the Ethernet management port is enabled. The switch cannot route packets from the Ethernet management port to a network port, and the reverse.

Even though the Ethernet management port does not support routing, you might need to enable routing protocols on the port (see Figure 1-4). For example, in Figure 1-4, you must enable routing protocols on the Ethernet management port when the PC is multiple hops away from the switch and the packets must pass through multiple Layer 3 devices to reach the PC.

Figure 1-4 Network Example with Routing Protocols Enabled

In **Figure 1-4**, if the Ethernet management port and the network ports are associated with the same routing process, the routes are propagated as follows:

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

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

Supported Features on the Ethernet Management Port

The Ethernet management port supports these features:

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

157551

**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 1-2](#) when using TFTP to download or upload a configuration file to the boot loader.

Table 1-2 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.
boot tftp: <i>/file-url ...</i>	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.
copy tftp: <i>/source-file-url filesystem:/destination-file-url</i>	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

These sections contain this configuration information:

- [Default Ethernet Interface Configuration](#), page 1-30
- [Configuring Interface Speed and Duplex Mode](#), page 1-31
- [Configuring IEEE 802.3x Flow Control](#), page 1-33
- [Configuring Auto-MDIX on an Interface](#), page 1-34
- [Configuring a Power Management Mode on a PoE Port](#), page 1-35
- [Budgeting Power for Devices Connected to a PoE Port](#), page 1-37
- [Configuring Power Policing](#), page 1-38
- [Adding a Description for an Interface](#), page 1-39

Default Ethernet Interface Configuration

Table 1-3 shows the Ethernet interface default configuration, including some features that apply only to Layer 2 interfaces. For more details on the VLAN parameters listed in the table, see [Chapter 1, “Configuring VLANs.”](#) For details on controlling traffic to the port, see [Chapter 1, “Configuring Port-Based Traffic Control.”](#)



Note

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

Table 1-3 *Default Layer 2 Ethernet Interface Configuration*

Feature	Default Setting
Operating mode	Layer 2 or switching mode (switchport command).
Allowed VLAN range	VLANs 1– 4094.
Default VLAN (for access ports)	VLAN 1 (Layer 2 interfaces only).
Native VLAN (for IEEE 802.1Q trunks)	VLAN 1 (Layer 2 interfaces only).
VLAN trunking	Switchport mode dynamic auto (supports DTP) (Layer 2 interfaces only).
Port enable state	All ports are enabled.
Port description	None defined.
Speed	Autonegotiate. (Not supported on the 10-Gigabit interfaces.)
Duplex mode	Autonegotiate. (Not supported on the 10-Gigabit interfaces.)
Flow control	Flow control is set to receive: off . It is always off for sent packets.
EtherChannel (PAgP)	Disabled on all Ethernet ports. See Chapter 1, “Configuring EtherChannels and Link-State Tracking.”

Table 1-3 Default Layer 2 Ethernet Interface Configuration (continued)

Feature	Default Setting
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked) (Layer 2 interfaces only). See the “ Configuring Port Blocking ” section on page 1-7.
Broadcast, multicast, and unicast storm control	Disabled. See the “ Default Storm Control Configuration ” section on page 1-3.
Protected port	Disabled (Layer 2 interfaces only). See the “ Configuring Protected Ports ” section on page 1-6.
Port security	Disabled (Layer 2 interfaces only). See the “ Default Port Security Configuration ” section on page 1-11.
Port Fast	Disabled. See the “ Default Optional Spanning-Tree Configuration ” section on page 1-12.
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).

Configuring Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, 1000, 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 include Gigabit Ethernet (10/100/1000-Mb/s) ports, 10-Gigabit Ethernet 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 1-31](#)
- [Setting the Interface Speed and Duplex Parameters, page 1-32](#)

Speed and Duplex Configuration Guidelines

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

- The 10-Gigabit Ethernet ports do not support the speed and duplex features. These ports operate only at 10,000 Mb/s and in full-duplex mode.
- 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.

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

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

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 3	speed { 10 100 1000 auto [10 100 1000] nonegotiate }	<p>This command is not available on a 10-Gigabit Ethernet interface.</p> <p>Enters the appropriate speed parameter for the interface:</p> <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. <p>For more information about speed settings, see the “Speed and Duplex Configuration Guidelines” section on page 1-31.</p>

	Command	Purpose
Step 4	<code>duplex {auto full half}</code>	This command is not available on a 10-Gigabit Ethernet interface. Enters the duplex parameter for the interface. Enables half-duplex mode (for interfaces operating only at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 Mb/s. You can configure the duplex setting when the speed is set to auto . For more information about duplex settings, see the “ Speed and Duplex Configuration Guidelines ” section on page 1-31.
Step 5	<code>end</code>	Returns to privileged EXEC mode.
Step 6	<code>show interfaces interface-id</code>	Displays the interface speed and duplex mode configuration.
Step 7	<code>copy running-config startup-config</code>	(Optional) Saves 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 100 Mb/s and the duplex mode to half on a 10/100/1000 Mb/s port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# speed 100
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 gigabitethernet1/0/2
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

Catalyst 3750-X or 3560-X ports can receive, but not send, pause frames.

You use the **flowcontrol** interface configuration command to set the interface’s ability to **receive** pause frames to **on**, **off**, or **desired**. 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.

To configure flow control on an interface, follow these steps beginning in privileged EXEC mode:

	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 10/100/1000-Mb/s and on 10/100/1000BASE-TX small form-factor pluggable (SFP)-module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

Table 1-4 shows the link states that result from auto-MDIX settings and correct and incorrect cabling.

Table 1-4 Link Conditions and Auto-MDIX Settings

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

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

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode
Step 2	interface <i>interface-id</i>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 3	speed auto	Configures the interface to autonegotiate speed with the connected device.
Step 4	duplex auto	Configures the interface to autonegotiate duplex mode with the connected device.
Step 5	end	Returns to privileged EXEC mode.
Step 6	show controllers ethernet-controller <i>interface-id</i> phy	Verifies the operational state of the auto-MDIX feature on the interface.
Step 7	copy running-config startup-config	(Optional) Saves 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

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.

Catalyst 3750-X switches also support StackPower, which allows switch power supplies to share the load across multiple systems in a stack by connecting up to four switches with power stack cables. See [Chapter 1, “Configuring Catalyst 3750-X StackPower”](#) for information on StackPower.

**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.

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

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i>	Specifies the physical port to be configured, and enter interface configuration mode.
Step 3	power inline { auto [max <i>max-wattage</i>] never static [max <i>max-wattage</i>] }	<p>Configures the PoE mode on the port. The keywords have these meanings:</p> <ul style="list-style-type: none"> • auto—Enables 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>—Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed. • never—Disables 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 linkup can occur, placing the port into the error-disabled state.</p> <ul style="list-style-type: none"> • static—Enables powered-device detection. Preallocate (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	Returns to privileged EXEC mode.
Step 5	show power inline [<i>interface-id</i> module <i>switch-number</i>]	<p>Displays PoE status for a switch or a switch stack for the specified interface or for a specified stack member.</p> <p>The module <i>switch-number</i> keywords are supported only on Catalyst 3750-X switches.</p>
Step 6	copy running-config startup-config	(Optional) Saves 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 1-13. For information about configuring voice VLAN, see [Chapter 1, “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 *CDP-specific* power consumption of the devices, and the switch adjusts the power budget accordingly. This 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 mW for the device, regardless of the CDP-specific amount of power needed. If the powered device reports a higher class than its CDP-specific 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** interface configuration command or the **power inline consumption default wattage** global 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.



Caution

You should carefully plan your switch power budget, enable the power monitoring feature, 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 Gi1/0/1: 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.
```

For more information about the IEEE power classifications, see the [“Power over Ethernet Ports” section on page 1-7](#).

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

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	no cdp run	(Optional) Disables CDP.
Step 3	power inline consumption default wattage	Configures the power consumption of powered devices connected to each the PoE port on the switch. The range for each device is 4000 to 15400 mW. The default is 15400 mW. Note When you use this command, we recommend you also enable power policing.
Step 4	end	Returns to privileged EXEC mode.

	Command	Purpose
Step 5	show power inline consumption default	Displays the power consumption status.
Step 6	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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

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

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	no cdp run	(Optional) Disables CDP.
Step 3	interface <i>interface-id</i>	Specifies the physical port to be configured, and enter interface configuration mode.
Step 4	power inline consumption <i>wattage</i>	Configures the power consumption of a powered device connected to a PoE port on the switch. The range for each device is 4000 to 15400 mW. The default is 15400 mW. Note When you use this command, we recommend you also enable power policing.
Step 5	end	Returns to privileged EXEC mode.
Step 6	show power inline consumption	Displays the power consumption data.
Step 7	copy running-config startup-config	(Optional) Saves 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 in the “Configuring Interface Characteristics” chapter of the software configuration guide for this release.

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

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

	Command	Purpose
Step 3	power inline police [action 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 <i>interval</i> 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 log keywords, the default action shuts down the port and puts the port in the error-disabled state.</p>
Step 4	exit	Returns to global configuration mode.
Step 5	errdisable detect cause inline-power and errdisable recovery cause inline-power and errdisable recovery interval <i>interval</i>	<p>(Optional) Enables error recovery from the PoE error-disabled state, and configures the PoE recover mechanism variables.</p> <p>By default, the recovery interval is 300 seconds.</p> <p>For interval <i>interval</i>, specify the time in seconds to recover from the error-disabled state. The range is 30 to 86400.</p>
Step 6	exit	Returns to privileged EXEC mode.
Step 7	show power inline police show errdisable recovery	Displays the power monitoring status, and verify the error recovery settings.
Step 8	copy running-config startup-config	(Optional) Saves 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.

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**.

To add a description for an interface, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i>	Specifies the interface for which you are adding a description, and enter interface configuration mode.
Step 3	description <i>string</i>	Adds a description (up to 240 characters) for an interface.
Step 4	end	Returns to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> description or show running-config	Verifies your entry.
Step 6	copy running-config startup-config	(Optional) Saves 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# configure 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 Interfaces



Note

Layer 3 interfaces are not supported on switches running the LAN Base feature set.

The switch supports these types of Layer 3 interfaces:

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



Note

When you create an SVI, it does not become active until it is associated with a physical port. For information about assigning Layer 2 ports to VLANs, see [Chapter 1, “Configuring VLANs.”](#)

When configuring SVIs, you can also configure SVI autostate exclude on a port in the SVI to exclude that port from being included in determining SVI line-state status. See the [“Configuring SVI Autostate Exclude”](#) section on page 1-42.

- Routed ports—Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command.

- Layer 3 EtherChannel ports—EtherChannel interfaces made up of routed ports.
EtherChannel port interfaces are described in [Chapter 1, “Configuring EtherChannels and Link-State Tracking.”](#)

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

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

- If you try to create a new routed port, the switch generates a message that there are not enough resources to convert the interface to a routed port, and the interface remains as a switch port.
- If you try to create an extended-range VLAN, an error message is generated, and the extended-range VLAN is rejected.
- If the switch is notified by VLAN Trunking Protocol (VTP) of a new VLAN, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.
- If the switch attempts to boot up with a configuration that has more VLANs and routed ports than hardware can support, the VLANs are created, but the routed ports are shut down, and the switch sends a message that this was due to insufficient hardware resources.

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.



Note

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

To configure a Layer 3 interface, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface { gigabitethernet <i>interface-id</i> } { vlan <i>vlan-id</i> } { port-channel <i>port-channel-number</i> }	Specifies the interface to be configured as a Layer 3 interface, and enter interface configuration mode.
Step 3	no switchport	For physical ports only, enters Layer 3 mode.
Step 4	ip address <i>ip_address subnet_mask</i>	Configures the IP address and IP subnet.
Step 5	no shutdown	Enables the interface.
Step 6	end	Returns to privileged EXEC mode.
Step 7	show interfaces [<i>interface-id</i>] show ip interface [<i>interface-id</i>] show running-config interface [<i>interface-id</i>]	Verifies the configuration.
Step 8	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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

This example shows how to configure a port as a routed port and to assign it an IP address:

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

Configuring SVI Autostate Exclude

Configuring SVI autostate exclude on an access or trunk port in an SVI excludes that port in the calculation of the status of the SVI line state (up or down) status even if it belongs to the same VLAN. When the excluded port is in the up state, and all other ports in the VLAN are in the down state, the SVI state is changed to down.

At least one port in the VLAN should be up and not excluded to keep the SVI state up. You can use this command to exclude the monitoring port status when determining the status of the SVI.

To exclude a port from SVI state-change calculations, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i>	Specifies a Layer 2 interface (physical port or port channel), and enter interface configuration mode.
Step 3	switchport autostate exclude	Excludes the access or trunk port when defining the status of an SVI line state (up or down).
Step 4	end	Returns to privileged EXEC mode.
Step 5	show running config interface <i>interface-id</i> show interface <i>interface-id</i> switchport	(Optional) Shows the running configuration. Verifies the configuration.
Step 6	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to configure an access or trunk port in an SVI to be excluded from the line-state status calculation:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport autostate exclude
Switch(config-if)# exit
```

Configuring the System MTU

The default maximum transmission unit (MTU) size for frames received and sent on all interfaces on the switch or switch stack is 1500 bytes. You can change the MTU size to support switched jumbo frames on all Gigabit Ethernet and 10-Gigabit Ethernet interfaces and to support routed frames on all routed ports.

- The system jumbo MTU value applies to switched packets on the Gigabit Ethernet and 10-Gigabit Ethernet ports of the switch or switch stack. Use the **system mtu jumbo bytes** global configuration command to specify the system jumbo MTU value.
- The system routing MTU value applies only to routed packets on all routed ports of the switch or switch stack. Use the **system mtu routing bytes** global configuration command to specify the system routing MTU value.

When configuring the system MTU values, follow these guidelines:

- The switch does not support the MTU on a per-interface basis.
- You can enter the **system mtu bytes** global configuration command on a Catalyst 3750-X switch, but the command does not take effect on the switch. This command only affects the system MTU size on Fast Ethernet ports on Catalyst 3750 members in a mixed hardware switch stack. In this stack, you can use the **system mtu bytes** global configuration command on a Catalyst 3750-X member to configure the system MTU size on a Catalyst 3750 member.
- The **system mtu**, **system mtu jumbo**, and **system mtu routing** global configuration commands do not take effect in these cases:
 - When you enter the **system mtu** command on a Catalyst 3750-X or 3560-X switch
 - In a mixed stack when you enter the **system mtu jumbo** command for the Fast Ethernet ports on a Catalyst 3750 member
 - When you enter the **system mtu routing** command on a switch on which only Layer 2 ports are configured



Note This command is not supported on switches running the LAN base feature set.

- When you use the **system mtu bytes** or **system mtu jumbo bytes** command to change the system MTU or system jumbo MTU size, you must reset the switch before the new configuration takes effect. The **system mtu routing** command does not require a switch reset to take effect.

The system MTU setting is saved in the switch environmental variable in NVRAM and becomes effective when the switch reloads. Unlike the system MTU routing configuration, the MTU settings you enter with the **system mtu** and **system mtu jumbo** commands are not saved in the switch Cisco IOS configuration file, even if you enter the **copy running-config startup-config** privileged EXEC command. Therefore, if you use TFTP to configure a new switch by using a backup configuration file and want the system MTU to be other than the default, you must explicitly configure the **system mtu** and **system mtu jumbo** settings on the new switch and then reload the switch.

In a switch stack, the MTU values applied to the members depend on the stack configuration:

- A stack consisting of only Catalyst 3750-X, Catalyst 3750-E, or Catalyst 3750 switches, also referred to as a Catalyst 3750-X-only, Catalyst 3750-X-only, or Catalyst 3750-only stack
- A stack consisting of Catalyst 3750-X and Catalyst 3750-E switches or either of these and Catalyst 3750 switches, also referred to as a mixed hardware stack

Table 1-5 shows how the MTU values are applied depending on the configuration.

Table 1-5 System MTU Values

Configuration	system mtu command	system jumbo mtu command	system routing mtu command
Standalone Catalyst 3750-X, 3750-E, 3560-X or 3560-E switch or Catalyst 3750-X-only or Catalyst 3750-E-only stack	You can enter the command on on a Catalyst 3750-X, Catalyst 3750-E, Catalyst 3560-X, or Catalyst 3560-E switch, but system MTU value does not take effect. ¹	Use the system mtu jumbo bytes command. The range is from 1500 to 9198 bytes.	Use the system mtu routing bytes command. The range is from 1500 to the system jumbo MTU value (in bytes). ²
Mixed hardware stack	Use the system mtu bytes command, which takes effect only on Catalyst 3750 members. ¹ The range is from 1500 to 1998 bytes.	Use the system mtu jumbo bytes command. The range is from 1500 to 9000 bytes.	Use the system mtu routing bytes command. The range is from 1500 to the system MTU value (in bytes). ²
Catalyst 3750-only stack Catalyst 3750 switch Catalyst 3560 switch	Use the system mtu bytes command. The range is from 1500 to 1998 bytes.	Use the system mtu jumbo bytes command. The range is from 1500 to 9000 bytes.	Use the system mtu routing bytes command. The range is from 1500 to the system MTU value (in bytes).

1. If you use the **system mtu bytes** command on a Catalyst 3750-X or 3750-E member in a mixed hardware stack, the setting takes effect on the Fast Ethernet ports of Catalyst 3750 members.
2. The system routing MTU value is the applied value, not the configured value.

The upper limit of the system routing MTU value is based on the switch or switch stack configuration and refers to either the currently applied system MTU or the system jumbo MTU value. For more information about setting the MTU sizes, see the **system mtu** global configuration command in the command reference for this release.

To change the MTU size for switched and routed packets, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	system mtu jumbo bytes	(Optional) Changes the MTU size for all Gigabit Ethernet and 10-Gigabit Ethernet interfaces on the switch or the switch stack. For information about the range for <i>bytes</i> , see Table 1-5 .
Step 3	system mtu routing bytes	(Optional) Changes the system MTU for routed ports. You can also set the maximum MTU to be advertised by the routing protocols that support the configured MTU size. The system routing MTU is the maximum MTU for routed packets and is also the maximum MTU that the switch advertises in routing updates for protocols such as OSPF. For information about the range for <i>bytes</i> , see Table 1-5 . Note This command is not supported on switches running the LAN base feature set.

	Command	Purpose
Step 4	<code>system mtu bytes</code>	(Optional) In a mixed hardware stack, change the MTU size for all Fast Ethernet interfaces on the Catalyst 3750 members. The range is 1500 to 1998 bytes; the default is 1500 bytes. Note This command does not apply to Catalyst 3560-X switches.
Step 5	<code>end</code>	Returns to privileged EXEC mode.
Step 6	<code>copy running-config startup-config</code>	Saves your entries in the configuration file.
Step 7	<code>reload</code>	Reloads the operating system.
Step 8	<code>show system mtu</code>	Verifies your settings.

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

This example shows how to set the maximum packet size for a Gigabit Ethernet port to 7500 bytes:

```
Switch(config)# system mtu jumbo 7500
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.
```

Configuring the Power Supplies

You can use the **power supply** user EXEC command to configure and manage the internal power supplies on the switch.

To configure and manage the internal power supplies, follow these steps beginning in user EXEC mode:

	Command	Purpose
Step 1	power supply <i>switch-number</i> {reset {hard soft} slot {A B} {off on}}	<p>Specifies a switch to reset or a power supply to set to off or on. By default, the switch power supply is on.</p> <ul style="list-style-type: none"> • reset—Resets the software or switch: <ul style="list-style-type: none"> – hard—Resets everything on the switch, including the hardware. – soft—Resets only the switch software. • slot A —Selects the power supply in slot A. • slot B —Selects power supply in slot B. <p>Note Power supply slot B slot is the closest to the outer edge of the switch.</p> <ul style="list-style-type: none"> • off—Sets the power supply off. • on—Sets the power supply on. <p>The <i>switch-number</i> is supported only on Catalyst 3750-X switches.</p>
Step 2	show env power	Verifies your settings.
Step 3	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

The switch does not support the **no power supply** user EXEC command. To return to the default setting, use the **power supply** *switch-number* slot {A | B} on command.

For more information about using the **power supply** user EXEC command, see the command reference for this release.

Configuring the Cisco RPS 2300 in a Mixed Stack

In a mixed stack with Catalyst 3750-X and 3750-E switches, one or more Catalyst 3750-E switches can be connected to a Cisco Redundant Power System 2300, also known as the RPS 2300. You can configure and manage an RPS 2300 connected to a Catalyst 3750-E switch in the stack.



Note

The Catalyst 3750-X and 3560-X switches do not have RPS connectors. These switches can be connected to an XPS-2200 expandable power supply (not available at this time). The Catalyst 3750-X switch also has stack power connectors. See [Chapter 1, “Configuring Catalyst 3750-X StackPower”](#) for information on stack power.

Follow these guidelines when configuring the RPS-2300:

- The RPS name is a 16-character-maximum string.
- In a switch stack, the RPS name applies to the RPS ports connected to the specified switch.
- If you do not want the RPS 2300 to provide power to a switch, but do not want to disconnect the RPS cable between the switch and the RPS 2300, use the **power rps switch-number port rps-port-id mode standby** user EXEC command.
- You can configure the priority of an RPS 2300 port from 1 to 6. Specifying a value of 1 assigns the port and its connected devices the highest priority and specifying a value of 6 assigns the port and its connected devices the lowest priority.

If multiple switches connected to the RPS 2300 need power, the RPS 2300 provides power to the switches with the highest priority. If the RPS 2300 still has power available, it can then provide power to the switches with lower priorities.

To configure and manage the RPS 2300, follow these steps beginning in user EXEC mode:

Command	Purpose
Step 1 power rps switch-number name {string serialnumber}	<p>Specifies the name of the RPS 2300.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> • switch-number—Specifies the stack member to which the RPS 2300 is connected. The range is 1 to 9, depending on the switch member numbers in the stack. This keyword is supported only on Catalyst 3750-E switches. • name—Sets the name of the RPS 2300 and enter one of these options: <ul style="list-style-type: none"> – string—Specifies the name such as <i>port1</i> or “<i>port 1</i>”. Using quotation marks before and after the name is optional, but you must use quotation marks if you want to include spaces in the port name. The name can have up to 16 characters. – serialnumber—Configures the switch to use the RPS 2300 serial number as the name.

	Command	Purpose
Step 2	power rps <i>switch-number</i> port <i>rps-port-id</i> mode { active standby }	<p>Specifies the mode of the RPS 2300 port.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> • <i>switch-number</i>—Specifies the stack member to which the RPS 2300 is connected. The range is 1 to 9, depending on the switch member numbers in the stack. This keyword is supported only on Catalyst 3750-E switches. • port <i>rps-port-id</i>—Specifies the RPS 2300 port. The range is from 1 to 6. • mode—Sets the mode of the RPS 2300 port: <ul style="list-style-type: none"> – active—The RPS 2300 can provide the power to a switch when the switch internal power supply cannot. – standby—The RPS 2300 is not providing power to a switch. <p>The default mode for RPS ports is active.</p>
Step 3	power rps <i>switch-number</i> port <i>rps-port-id</i> priority <i>priority</i>	<p>Sets the priority of the RPS 2300 port. The range is from 1 to 6, where 1 is the highest priority and 6 is the lowest priority.</p> <p>The default port priority is 6.</p>
Step 4	show env rps	Verifies your settings.
Step 5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

To return to the RPS 2300 default settings, use these commands:

- To return to the default name setting (no name is configured), use the **power rps** *switch-number* **port** *rps-port-id* **name** user EXEC command with no space between the quotation marks.
- To return to the default port mode, use the **power rps** *switch-number* **port** *rps-port-id* **active** command.
- To return to the default port priority, use the **power rps** *switch-number* **port** *rps-port-id* **priority** command.

For more information about using the **power rps** user EXEC command, see the command reference for this release.

Configuring the Cisco eXpandable Power System (XPS) 2200

The Cisco XPS 2200 is a standalone power system that you can connect to Catalyst 3560-X and Catalyst 3750-X switches to provide backup power to connected devices or, in a Catalyst 3750-X power stack, to supply additional power to the power stack budget. The XPS 2200 power ports and internal power supplies can operate in redundant power supply (RPS) mode or stack power (SP) mode.

For more information about the XPS 2000, see the configuration notes:

http://preview.cisco.com/en/US/docs/switches/power_supplies/xps2200/software/configuration/note/ol24241.html

You use the switch CLI to configure the XPS:

- [Configuring the System Names, page 1-49](#)
- [Configuring XPS Ports, page 1-50](#)
- [Configuring XPS Power Supplies, page 1-51](#)

Configuring the System Names

To configure a name for the XPS 2200 system and for an XPS port connected to a switch, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	power xps <i>switch-number</i> name {<i>name</i> <i>serialnumber</i>}	Configures a name for the XPS 2200 system. <ul style="list-style-type: none"> • <i>name</i>—Enter a name for the XPS 2000 port. The name can have up to 20 characters. • serialnumber—Use the serial number of the XPS 2200 as the system name. <p>The <i>switch-number</i> appears only on Catalyst 3750-X switches and represents the switch number in the data stack, a value from 1 to 9.</p>
Step 3	power xps <i>switch-number</i> port {<i>name</i> <i>hostname</i> <i>serialnumber</i>}	Configures a name for an XPS 2200 port connected to the switch. <ul style="list-style-type: none"> • <i>name</i>—Enter a name for the XPS 2000 port. • hostname—Use the hostname of the switch connected to the port. • serialnumber—Use the serial number of the switch connected to the port. <p>The <i>switch-number</i> appears only on Catalyst 3750-X switches and represents the switch number in the data stack, a value from 1 to 9.</p>
Step 4	end	Returns to privileged EXEC mode.
Step 5	show env xps system	Verifies the configured name of the system and ports.
Step 6	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Use the **no power xps *switch-number* name** command to remove the system name. Use the **no power xps *switch-number* port** command to remove the port name.

Configuring XPS Ports

These commands apply to the XPS and are saved in the XPS, but the configuration is not saved in the switch configuration file.

To configure XPS 2200 ports, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	power xps <i>switch-number</i> port { <i>number</i> connected } mode { disable enable }	<p>Sets the port to be enabled or disabled.</p> <ul style="list-style-type: none"> <i>number</i>—Enter the XPS 2200 port number. The range is 1 to 9. connected—Enter this keyword if you do not know the port number to which the switch is connected. mode disable—Disables (shut down) the XPS port. <p>Note Disabling an XPS port is like removing the cable and appears the same in the show command outputs. If the physical cable is connected, you can still use the enable keyword to enable the port.</p> <ul style="list-style-type: none"> mode enable—Enables the XPS port. This is the default. <p>The <i>switch-number</i> appears only on Catalyst 3750-X switches and represents the switch number in the data stack, a value from 1 to 9.</p>
Step 2	power xps <i>switch-number</i> port { <i>number</i> connected } role { auto rps }	<p>Sets the role of the XPS port.</p> <ul style="list-style-type: none"> role auto—The port mode is determined by the switch connected to the port. This is the default. When a Catalyst 3560-X switch or Catalyst 3750-X switch running the LAN base image is connected, the mode is RPS. When a Catalyst-3750-X switch is connected, the mode is stack power (SP). role RPS—The XPS acts as a back up if the switch power supply fails. At least one RPS power supply must be in RPS mode for this configuration. <p>The <i>switch-number</i> appears only on Catalyst 3750-X switches and represents the switch number in the data stack, a value from 1 to 9.</p> <p>The default role for a port is Auto-SP, where the power mode is determined by the switch connected to the port (RPS for Catalyst 3560-X or Catalyst 3750-X switches running the LAN base image, or SP for Catalyst 3750-X switches running the IP base or IP services image).</p>
Step 3	power xps <i>switch-number</i> port { <i>number</i> connected } priority <i>port-priority</i>	<p>Sets the RPS priority of the port, where higher priority ports take precedence over low priority ports if multiple power supplies fail. This command takes effect only when the port mode is RPS. When the port mode is stack power, you set priority by using the stack power commands.</p> <ul style="list-style-type: none"> priority <i>port-priority</i>—Sets the RPS priority of the port. The range is 1 to 9, with 1 being the highest priority. The default priority is the XPS port number. <p>The <i>switch-number</i> appears only on Catalyst 3750-X switches and represents the switch number in the data stack, a value from 1 to 9.</p>
Step 4	show env xps port	Verifies the XPS configuration of the port.

For auto-SP ports participating in stack power, configure stack power characteristics by using the stack power commands described in [Chapter 1, “Configuring Catalyst 3750-X StackPower.”](#)

Configuring XPS Power Supplies

You can configure the mode of an XPS power supply and you can configure it to be on or off. To configure XPS 2200 power supplies. Follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	<code>power xps <i>switch-number</i> supply {A B} mode {rps sp}</code>	<p>Sets the XPS power supply mode.</p> <ul style="list-style-type: none"> supply {A B}—Selects the power supply to configure. Power supply A is on the left (labeled PS1) and power supply B (PS2) is on the right. mode rps—Sets the power supply mode to RPS, to back up connected switches. This is the default setting for power supply A (PS1). mode sp—Sets the power supply mode to stack power (SP), to participate in the power stack. This is the default setting for power supply B (PS2). <p>The <i>switch-number</i> appears only on Catalyst 3750-X switches and represents the switch number in the data stack, a value from 1 to 9.</p>
Step 2	<code>power xps <i>switch-number</i> supply {A B} {on off}</code>	<p>Sets the XPS power supply to be on or off. The default is for both power supplies to be on.</p> <p>The <i>switch-number</i> appears only on Catalyst 3750-X switches and represents the switch number in the data stack, a value from 1 to 9.</p>
Step 3	<code>end</code>	Returns to privileged EXEC mode.
Step 4	<code>show env xps power</code>	Displays the status of the XPS power supplies.

Monitoring and Maintaining the Interfaces

These sections contain interface monitoring and maintenance information:

- [Monitoring Interface Status, page 1-52](#)
- [Clearing and Resetting Interfaces and Counters, page 1-53](#)
- [Shutting Down and Restarting the Interface, page 1-53](#)

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 1-6 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*.

Table 1-6 Show Commands for Interfaces

Command	Purpose
show env power switch [<i>switch-number</i>]	(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch. The range is 1 to 9, depending on the switch member numbers in the stack. These keywords are available only on Catalyst 3750-E switches.
show env rps	Displays whether a redundant power system (RPS) is connected to the switch as follows: <ul style="list-style-type: none"> – Catalyst 3750-E or 3560-E switch—Cisco Redundant Power System 2300, also referred to as the RPS 2300. – Catalyst 3750v2 or 3560v2 switch—Cisco Redundant Power System 2300. – Catalyst 3750, 3560, 2970, or 2960 switches—RPS 2300 or Cisco RPS 675 Redundant Power System, also referred to as the RPS 675.
show env rps detail	(Optional) Displays the details about the RPSs that are connected to the switch or switch stack.
show env rps switch [<i>switch-number</i>]	(Optional) Displays the RPSs that are connected to each switch in the stack or to the specified switch. The range is 1 to 9, depending on the switch member numbers in the stack.
show interfaces [<i>interface-id</i>]	Displays the status and configuration of all interfaces or a specific interface.
show interfaces interface-id status [err-disabled]	Displays interface status or a list of interfaces in the error-disabled state.
show interfaces [<i>interface-id</i>] switchport	Displays administrative and operational status of switching (nonrouting) ports. You can use this command to find out if a port is in routing or in switching mode.
show interfaces [<i>interface-id</i>] description	Displays the description configured on an interface or all interfaces and the interface status.
show ip interface [<i>interface-id</i>]	Displays the usability status of all interfaces configured for IP routing or the specified interface.
show interface [<i>interface-id</i>] stats	Displays the input and output packets by the switching path for the interface.
show interfaces interface-id	(Optional) Displays speed and duplex on the interface.
show interfaces transceiver dom-supported-list	(Optional) Displays Digital Optical Monitoring (DOM) status on the connect SFP modules.

Table 1-6 Show Commands for Interfaces (continued)

Command	Purpose
show interfaces transceiver properties	(Optional) Displays temperature, voltage, or amount of current on the interface.
show interfaces [<i>interface-id</i>] [{ transceiver properties detail }] [<i>module number</i>]	Displays physical and operational status about an SFP module.
show running-config interface [<i>interface-id</i>]	Displays the running configuration in RAM for the interface.
show version	Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images.
show controllers ethernet-controller <i>interface-id</i> phy	Displays the operational state of the auto-MDIX feature on the interface.
show power inline [<i>interface-id</i> module switch-number]	Displays PoE status for a switch or switch stack, for an interface, or for a specific switch in the stack.
show power inline consumption	Displays the power consumption data.
show power inline police	Displays the power policing data.

Clearing and Resetting Interfaces and Counters

Table 1-7 lists the privileged EXEC mode **clear** commands that you can use to clear counters and reset interfaces.

Table 1-7 Clear Commands for Interfaces

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

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.

To shut down an interface, follow these steps beginning in privileged EXEC mode:

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface { vlan <i>vlan-id</i> } { gigabitethernet <i>interface-id</i> } { port-channel <i>port-channel-number</i> }	Selects the interface to be configured.
Step 3	shutdown	Shuts down an interface.
Step 4	end	Returns to privileged EXEC mode.
Step 5	show running-config	Verifies your entry.

Use the **no shutdown** interface configuration command to restart the interface.

To verify that an interface is disabled, enter the **show interfaces** privileged EXEC command. A disabled interface is shown as *administratively down* in the display.