



CHAPTER 15

Configuring Interface Characteristics

Finding Feature Information

Your software release may not support all the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release.

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

Restrictions for Configuring Interface Characteristics

- The EtherChannel port group interface is supported on a switch running the LAN Base image.

Information About Configuring Interface Characteristics

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.

- [Port-Based VLANs, page 15-2](#)
- [Switch Ports, page 15-2](#)
- [Access Ports, page 15-3](#)
- [Trunk Ports, page 15-4](#)
- [EtherChannel Port Groups, page 15-4](#)
- [Dual-Purpose Uplink Ports, page 15-4](#)
- [Connecting Interfaces, page 15-5](#)

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 the [Chapter 17, “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.

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 4096), 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.

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

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

Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. 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. Switch ports are used for managing the physical interface and associated Layer 2 protocols.

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 17, “Configuring VLANs.”](#)

Routed Ports

**Note**

The LAN base image supports static routing.

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. Routed ports are supported only on switches running the IP base or IP services image.

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.

For more information about IP unicast routing and routing protocols, see [Chapter 41, “Configuring Static IP Unicast Routing”](#)

Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port.

If an access port receives an 802.1Q tagged packet, the packet is dropped, and the source address is not learned.

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 Authentication with VLAN Assignment” section on page 13-15](#).
- 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 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 19, “Configuring Voice VLAN.”](#)

Trunk Ports

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

The switch supports only IEEE 802.1Q trunk ports. 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 4096) 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 17, “Configuring VLANs.”](#)

EtherChannel Port Groups



Note

The LAN Base image supports EtherChannel port groups.

EtherChannel port groups treat multiple switch ports as one switch port. These port groups act as a single logical port for high-bandwidth connections between switches or between switches and servers. An EtherChannel balances the traffic load across the links in the channel. If a link within the EtherChannel fails, traffic previously carried over the failed link changes to the remaining links. You can group multiple trunk ports into one logical trunk port or group multiple access ports into one logical access port.

Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. 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. 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 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 more information, see [Chapter 40, “Configuring EtherChannels.”](#)

Dual-Purpose Uplink Ports

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

By default, the switch dynamically selects the interface type that first links up. However, you can use the **media-type** interface configuration command to manually select the RJ-45 connector or the SFP module connector. To return to the default setting, use the **media-type auto interface** or the **no media-type** interface configuration commands.

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

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

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

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

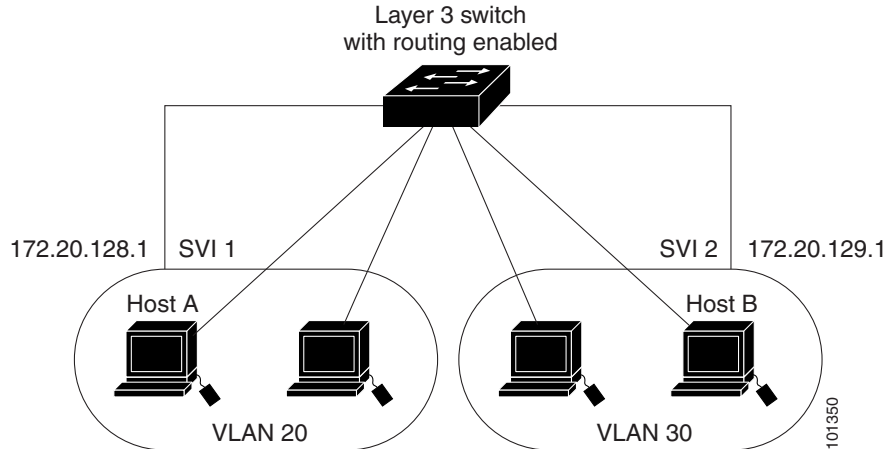
- When the 100BASE-*x* SFP module is inserted into the module slot and there is no link on the RJ-45 side, the switch disables the RJ-45 interface and selects the SFP module interface. This is the behavior even if there is no cable connected and if there is no link on the SFP module side.
- When the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

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

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 15-1](#)).

Figure 15-1 Connecting VLANs with a Layer 3 Switch

Basic routing (static routing and RIP) is supported on the LAN base image. Whenever possible, to maintain high performance, forwarding is done by the switch hardware. However, only IP Version 4 packets with Ethernet II encapsulation can be routed in hardware. *Non-IP traffic and traffic with other encapsulation methods can be fallback-bridged by hardware.*

The routing function can be enabled on all SVIs. The switch routes only IP traffic. When IP routing protocol parameters and address configuration are added to an SVI, any IP traffic received from these ports is routed. For more information, see [Chapter 41, “Configuring Static IP Unicast Routing.”](#)

- *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. When configuring fallback bridging, you assign SVIs to bridge groups with each SVI assigned to only one bridge group. All interfaces in the same group belong to the same bridge domain.*

Using Interface Configuration Mode

The switch supports these interface types:

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

You can also configure a range of interfaces (see the [“Configuring a Range of Interfaces”](#) section on page 15-13).

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

- **Type**—*Port types depend on those supported on the switch. Possible types are Fast Ethernet (fastethernet or fa) for 10/100 Mb/s Ethernet, Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000 Mb/s Ethernet ports, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces.*
- **Port number**—The physical interface number on the switch. The port numbers for the IE-2000-4TC switch model are 1–4 for the Fast Ethernet ports and 1–2 for the Gigabit Ethernet ports. The port numbers for the IE-2000-8TC switch model are 1–8 for the Fast Ethernet ports and 1–2 for the Gigabit Ethernet ports. [Table 15-1](#) shows the switch and module combinations and the interface

numbers.

Table 15-1 *Switch Interface Numbers*

Switch Model	Interface Numbering Scheme
IE-2000-4TS-L switch	Fast Ethernet1/1, Fast Ethernet1/2, Fast Ethernet1/3, Fast Ethernet1/4, Gigabit Ethernet1/1, and Gigabit Ethernet1/2
IE-2000-4TS-B switch	Fast Ethernet1/1, Fast Ethernet1/2, Fast Ethernet1/3, Fast Ethernet1/4, Gigabit Ethernet1/1, and Gigabit Ethernet1/2
IE-2000-4T-L switch	Fast Ethernet1/1, Fast Ethernet1/2, Fast Ethernet1/3, Fast Ethernet1/4, Gigabit Ethernet1/1, and Gigabit Ethernet1/2
IE-2000-4T-B switch	Fast Ethernet1/1, Fast Ethernet1/2, Fast Ethernet1/3, Fast Ethernet1/4, Gigabit Ethernet1/1, and Gigabit Ethernet1/2
IE-2000-4TS-G--L switch	Fast Ethernet1/1, Fast Ethernet1/2, Fast Ethernet1/3, Fast Ethernet1/4, Gigabit Ethernet1/1, and Gigabit Ethernet1/2
IE-2000-4TS-G-B switch	Fast Ethernet1/1, Fast Ethernet1/2, Fast Ethernet1/3, Fast Ethernet1/4, Gigabit Ethernet1/1, and Gigabit Ethernet1/2
IE-2000-8TC-L switch	Fast Ethernet1/1, Fast Ethernet1/2, Fast Ethernet1/3, Fast Ethernet1/4, Fast Ethernet1/5, Fast Ethernet1/6, Fast Ethernet1/7, Fast Ethernet1/8, Gigabit Ethernet1/1, and Gigabit Ethernet1/2
IE-2000-8TC-B switch	Fast Ethernet1/1, Fast Ethernet1/2, Fast Ethernet1/3, Fast Ethernet1/4, Fast Ethernet1/5, Fast Ethernet1/6, Fast Ethernet1/7, Fast Ethernet1/8, Gigabit Ethernet1/1, and Gigabit Ethernet1/2
	Fast Ethernet2/1, Fast Ethernet2/2, Fast Ethernet2/3, Fast Ethernet2/4, Fast Ethernet2/5, Fast Ethernet2/6, Fast Ethernet2/7, and Fast Ethernet2/8
	Fast Ethernet3/1, Fast Ethernet3/2, Fast Ethernet3/3, Fast Ethernet3/4, Fast Ethernet3/5, Fast Ethernet3/6, Fast Ethernet3/7, and Fast Ethernet3/8

You can identify physical interfaces by looking at the switch. You can also use the **show** privileged EXEC commands to display information about a specific interface or all the interfaces.

Default Ethernet Interface Settings

For more details on the VLAN parameters listed in the table, see [Chapter 17, “Configuring VLANs.”](#) For details on controlling traffic to the port, see [Chapter 29, “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 15-2 Default Layer 2 Ethernet Interface Settings

Feature	Default Setting
Operating mode	Layer 2 or switching mode (switchport command).
Allowed VLAN range	VLANs 1 to 4096.
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	Switch port mode dynamic auto (supports DTP) (Layer 2 interfaces only).
Port enable state	All ports are enabled.
Port description	None defined.
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
Flow control	Flow control is set to receive: off . It is always off for sent packets.
EtherChannel (PAgP)	Disabled on all Ethernet ports. Chapter 40, “Configuring EtherChannels.”
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked) (Layer 2 interfaces only).
Broadcast, multicast, and unicast storm control	Disabled.
Protected port	Disabled (Layer 2 interfaces only).
Port security	Disabled (Layer 2 interfaces only).
Port Fast	Disabled.
Auto-MDIX	Enabled. Note The switch might not support a prestandard powered device—such as Cisco IP phones and access points that do not fully support IEEE 802.3af—if that powered device is connected to the switch through a crossover cable. This is regardless of whether auto-MDIX is enabled on the switch port.
Keepalive messages	Disabled on SFP module ports; enabled on all other ports.

Interface Speed and Duplex Mode

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

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

Speed and Duplex Configuration Guidelines

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

- Fast Ethernet (10/100-Mb/s) ports support all speed and duplex options.
- Gigabit Ethernet (10/100/1000-Mb/s) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mb/s do not support half-duplex mode.
- For SFP module ports, the speed and duplex CLI options change depending on the SFP module type:
 - The 1000BASE-*x* (where *x* is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the **nonegotiate** keyword in the **speed** interface configuration command. Duplex options are not supported.
 - The 1000BASE-T SFP module ports support the same speed and duplex options as the 10/100/1000-Mb/s ports.
 - The 100BASE-*x* (where *x* is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support only 100 Mb/s. These modules support full- and half- duplex options but do not support autonegotiation.

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

- If both ends of the line support autonegotiation, we highly recommend the default setting of **auto** negotiation.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- When STP is enabled and a port is reconfigured, the switch can take up to 30 seconds to check for loops. The port LED is amber while STP reconfigures.



Caution

Changing the interface speed and duplex mode configuration might shut down and reenables the interface during the reconfiguration.

IEEE 802.3x Flow Control

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

**Note**

Ports on the switch can receive, but not send, pause frames.

You use the **flowcontrol** interface configuration command to set the interface's ability to **receive** pause frames to **on**, **off**, or **desired**. The default state is **off**.

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

These rules apply to flow control settings on the device:

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

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. When you enable auto-MDIX, you must also set the interface speed and duplex to **auto** so that the feature operates correctly.

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

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 (up or down line state) 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 line state up. You can use this command to exclude the monitoring port status when determining the status of the SVI.

System MTU

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

You can change the MTU size for routed ports by using the **system mtu routing** global configuration command.

**Note**

You cannot configure a routing MTU size that exceeds the system MTU size. If you change the system MTU size to a value smaller than the currently configured routing MTU size, the configuration change is accepted, but not applied until the next switch reset. When the configuration change takes effect, the routing MTU size automatically defaults to the new system MTU size.

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

You cannot set the MTU size for an individual interface; you set it for all 10/100 or all Gigabit Ethernet interfaces. When you change the system or jumbo MTU size, you must reset the switch before the new configuration takes effect. The **system mtu routing** command does not require a switch reset to take effect.

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

Routed packets are subjected to MTU checks on the output ports. The MTU value used for routed ports is derived from the applied **system mtu** value (not the **system mtu jumbo** value). That is, the routed MTU is never greater than the system MTU for any VLAN. The routing protocols use the system MTU value when negotiating adjacencies and the MTU of the link. For example, the Open Shortest Path First (OSPF) protocol uses this MTU value before setting up an adjacency with a peer router. To view the MTU value for routed packets for a specific VLAN, use the **show platform port-asic mvid** privileged EXEC command.

**Note**

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

How to Configure Interface Characteristics

Configuring Layer 3 Interfaces

The switch supports these types of Layer 3 interfaces:

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

**Note**

When you create an SVI, it does not become active until it is associated with a physical port. For information about assigning Layer 2 ports to VLANs, see [Chapter 17, “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 15-17.

- 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 40, “Configuring EtherChannels.”](#)

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. 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 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 switchport.
- 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 re-enables the interface, which might generate messages on the device to which the interface is connected. Furthermore, when you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface {{fastethernet 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 enters interface configuration mode.
Step 3	no switchport	For physical ports only, enter 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.

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

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



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

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

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

Step 4 After you configure an interface, verify its status by using the **show** privileged EXEC commands listed in the [“Monitoring and Maintaining Interface Characteristics”](#) section on page 15-18.

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.

Interface Range Restrictions

- When you use the **interface range** command with port channels, the first and last port-channel number must be active port channels.
- 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 as in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs), but you can combine multiple interface types in a macro.

	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 enters interface-range configuration mode. <ul style="list-style-type: none"> • interface range—Configures up to five port ranges or a previously defined macro. • macro <i>macro_name</i>—Specifies the 32-character maximum character string. • 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		Uses 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.

Configuring and Using Interface Range Macros

Before You Begin

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.

	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"> • macro <i>macro_name</i>—Specifies the 32-character maximum character string. • A macro can contain up to five comma-separated interface ranges. • <i>interface-range</i>—Consists 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.

	Command	Purpose
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>show running-config include define</code>	Shows the defined interface range macro configuration.

Configuring Ethernet Interfaces

Setting the Type of a Dual-Purpose Uplink Port

Perform this task to select which dual-purpose uplink to activate so that you can set the speed and duplex. This procedure is optional.

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface <i>interface-id</i></code>	Specifies the dual-purpose uplink port to be configured, and enters interface configuration mode.
Step 3	<code>media-type { auto-select rj45 sfp }</code>	<p>Selects the interface and type of a dual-purpose uplink port. The keywords have these meanings:</p> <ul style="list-style-type: none"> auto-select—The switch dynamically selects the type. When link up is achieved, the switch disables the other type until the active link goes down. When the active link goes down, the switch enables both types until one of them links up. In auto-select mode, the switch configures both types with autonegotiation of speed and duplex (the default). Depending on the type of installed SFP module, the switch might not be able to dynamically select it. rj45—The switch disables the SFP module interface. If you connect an SFP module to this port, it cannot attain a link even if the RJ-45 side is down or is not connected. In this mode, the dual-purpose port behaves like a 10/100/1000BASE-TX interface. You can configure the speed and duplex settings consistent with this interface type. sfp—The switch disables the RJ-45 interface. If you connect a cable to the RJ-45 port, it cannot attain a link even if the SFP module side is down or if the SFP module is not present. Based on the type of installed SFP module, you can configure the speed and duplex settings consistent with this interface type.
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>show interfaces <i>interface-id</i> transceiver properties</code>	Verifies your setting.

Setting the Interface Speed and Duplex Parameters

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface interface-id</code>	Specifies the physical interface to be configured, and enters interface configuration mode.
Step 3	<code>speed {10 100 1000 auto [10 100 1000] nonegotiate}</code>	Enters the appropriate speed parameter for the interface: <ul style="list-style-type: none"> • 10, 100, or 1000—Sets a specific speed for the interface. The 1000 keyword is available only for 10/100/1000 Mb/s ports. • auto—Enables 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. • nonegotiate—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.
Step 4	<code>duplex {auto full half}</code>	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.
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.

Configuring IEEE 802.3x Flow Control

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface interface-id</code>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 3	<code>flowcontrol {receive} {on off desired}</code>	Configures the flow control mode for the port.
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>show interfaces interface-id</code>	Verifies the interface flow control settings.

Configuring Auto-MDIX on an Interface

	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 enters 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	mdix auto	Enables auto-MDIX on the interface.
Step 6	end	Returns to privileged EXEC mode.
Step 7	show controllers ethernet-controller <i>interface-id phy</i>	Verifies the operational state of the auto-MDIX feature on the interface.

Adding a Description for an Interface

	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 enters 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.

Configuring SVI Autostate Exclude

	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 enters 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.

Configuring the System MTU

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>system mtu bytes</code>	(Optional) Changes the MTU size for all interfaces on the switch that are operating at 10 or 100 Mb/s. The range is 1500 to 1998 bytes; the default is 1500 bytes.
Step 3	<code>system mtu jumbo bytes</code>	(Optional) Changes the MTU size for all Gigabit Ethernet interfaces on the switch. The range is 1500 to 9000 bytes; the default is 1500 bytes.
Step 4	<code>system mtu routing bytes</code>	(Optional) Changes the system MTU for routed ports. The range is 1500 to the system MTU value, the maximum MTU that can be routed for all ports. Although larger packets can be accepted, they cannot be routed.
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>	(Optional) Verifies your settings.

Monitoring and Maintaining Interface Characteristics

Monitoring Interface Status

Table 15-3 Show Commands for Interfaces

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

Table 15-3 Show Commands for Interfaces (continued)

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

Clearing and Resetting Interfaces and Counters

Table 15-4 Clear Commands for Interfaces

Command	Purpose
<code>clear counters [interface-id]</code>	Clears interface counters. Note This command does not clear counters retrieved by using Simple Network Management Protocol (SNMP), but only those seen with the show interface privileged EXEC command.
<code>clear interface interface-id</code>	Resets the hardware logic on an interface.
<code>clear line [number console 0 vty number]</code>	Resets the hardware logic on an asynchronous serial line.

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.

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface {vlan vlan-id} {{fastethernet gigabitethernet} interface-id} {port-channel port-channel-number}</code>	Selects the interface to be configured.

	Command	Purpose
Step 3	<code>shutdown</code>	Shuts down an interface. Note Use the no shutdown interface configuration command to restart the interface.
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>show running-config</code>	Verifies your entry.

Configuration Examples for Configuring Interface Characteristics

Configuring the Interface Range: Examples

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

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

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

```
Switch# configure terminal
Switch(config)# interface range fastethernet1/1 - 3, gigabitethernet1/1 - 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 Interface Range Macros: Examples

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

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

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

```
Switch# configure terminal
Switch(config)# define interface-range macro1 fastethernet1/1 - 2, gigabitethernet1/1 - 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#
```

Setting Speed and Duplex Parameters: Example

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

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

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

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

Enabling auto-MDIX: Example

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

```
Switch# configure terminal
Switch(config)# interface gigabitetherenet1/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

Adding a Description on a Port: Example

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

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitetherenet1/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitetherenet1/2 description
Interface Status      Protocol Description
Gi1/2    admin down    down    Connects to Marketing
```

Configuring SVI Autostate Exclude: Example

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

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

Additional References

The following sections provide references related to switch administration:

Related Documents

Related Topic	Document Title
Cisco IE 2000 commands	<i>Cisco IE 2000 Switch Command Reference</i> , Release 15.0(1)EY
Cisco IOS basic commands	<i>Cisco IOS Configuration Fundamentals Command Reference</i>
Cisco IOS interface commands	<i>Cisco IOS Interface Command Reference</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

