



Configuring Interface Characteristics

This chapter defines the types of interfaces on the switch and describes how to configure them. The chapter has these sections:

- [Understanding Interface Types, page 7-1](#)
- [Using the Interface Command, page 7-7](#)
- [Configuring Layer 2 Interfaces, page 7-12](#)
- [Monitoring and Maintaining the Layer 2 Interface, page 7-16](#)
- [Configuring Layer 3 Interfaces, page 7-21](#)



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 3550 Multilayer Switch Command Reference* for this release and the online *Cisco IOS Interface Command Reference for Release 12.1*.

Understanding Interface Types

This section describe 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.

These sections are included:

- [Port-Based VLANs, page 7-2](#)
- [Switch Ports, page 7-2](#)
- [EtherChannel Port Groups, page 7-3](#)
- [Switch Virtual Interfaces, page 7-4](#)
- [Routed Ports, page 7-4](#)
- [Connecting Interfaces, page 7-5](#)

Port-Based VLANs

A Virtual LAN (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 8, “Creating and Maintaining 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 VLAN Trunk Protocol (VTP) learns of its existence from a neighbor on a trunk, or when a user adds a VLAN to the local VTP database.

To configure VLANs, use the **vlan database** privileged EXEC command to enter VLAN configuration mode.

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

Configure switch ports (access ports and trunk ports) by using the switchport interface configuration commands. For detailed information about configuring access ports and trunk ports, see [Chapter 8, “Creating and Maintaining VLANs.”](#)

Access Ports

An access port carries the traffic of and belongs to only one VLAN. Traffic is received and transmitted 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 802.1Q tagged), the packet is dropped, the source address is not learned, and the frame is counted in the *No destination* statistic.

Two types of access ports are supported:

- Static access ports are manually assigned to a VLAN.
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is a member of no VLAN, and forwarding to and from the port is only enabled after the VLAN membership of the port is discovered. In the Catalyst 3550 switch, dynamic access ports are assigned to a VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6000 series switch; the Catalyst 3550 switch does not support the function of a VMPS.

Trunk Ports

A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. Two types of trunk ports 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 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 transmitted untagged. All other traffic is transmitted 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 1005) are in the allowed list. A trunk port can only become a member of a VLAN if VTP knows of the VLAN and 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.

**Note**

VLAN 1 cannot be excluded from the allowed list.

For more information about trunk ports, see [Chapter 8, “Creating and Maintaining VLANs.”](#)

EtherChannel Port Groups

EtherChannel port groups provide the ability to 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. All protocols except DTP, Cisco Discovery Protocol (CDP), and Port Aggregation Protocol (PAgP) operate only on aggregated switch ports and are not aware of the physical ports within the port group.

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. For Layer 2 interfaces, the logical interface is dynamically created. For both Layer 3 and 2 interfaces, you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command. This command binds the physical and logical ports together. For more information, see [Chapter 19, “Configuring EtherChannel.”](#)

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 it is only necessary to configure an SVI for a VLAN when you wish to route between VLANs, 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. In Layer 2 mode, SVIs provide IP host connectivity only to the system; in Layer 3 mode, you can configure routing across SVIs.

To use SVIs in Layer 3 mode, you must have the enhanced multilayer switch image installed on your switch.



Note

In its default state, the switch supports up to 1005 VLANs, but we recommend a maximum of 256 simultaneously active VLANs to ensure sufficient system memory resources to support features enabled in the VLANs. However, there are four available switch database management (SDM) templates that you can use to reallocate system resources, depending on your application. Refer to the [“Optimizing System Resources for User-Selected Features” section on page 6-41](#) for more information about the templates.

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 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 [“Configuring IP Addressing” section on page 20-4](#).

SVIs support routing protocol and bridging configurations. For more information about configuring IP routing, see [Chapter 20, “Configuring IP Unicast Routing,”](#) and [Chapter 24, “Configuring Fallback Bridging.”](#)

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.



Note

To configure routed ports, you must have the enhanced multilayer switch image installed on your switch.

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 **configure ip routing** and **configure router protocol** commands.



Caution

Entering a **no switchport** command shuts the interface down and then reenables it, which might generate messages on the device to which the interface is connected. In addition, when you use this command to put the interface into Layer 3 mode, you are deleting any Layer 2 characteristics configured on the interface.

On a Catalyst 3550-12T switch, we recommend configuring a maximum total of 16 routed interfaces (SVIs and routed ports) simultaneously to allow enough system resources to support features enabled on these interfaces. If requirements exceed the system hardware allocation, processing overflow is sent to the CPU, degrading performance. Refer to the [“Optimizing System Resources for User-Selected Features” section on page 6-41](#) for more information about feature combinations.

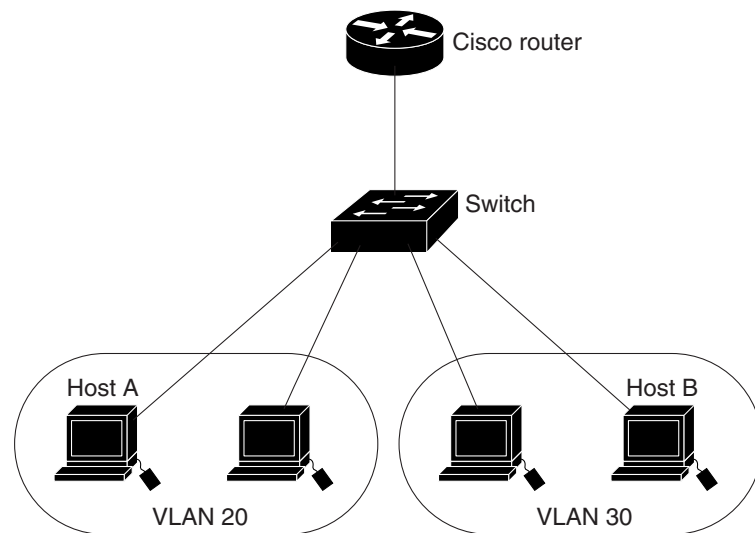
For more information about IP unicast routing and routing protocols, see [Chapter 20, “Configuring IP Unicast Routing.”](#)

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 or interface.

With a standard Layer 2 switch, ports in different VLANs have to exchange information through a router. In the configuration shown in [Figure 7-1](#), when Host A in VLAN 20 sends data to Host B in VLAN 30, it must go from Host A to the switch, to the router, back to the switch, and then to Host B.

Figure 7-1 Connecting VLANs with Layer 2 Switches



By using the Catalyst 3550 with the enhanced multilayer switch image installed, when you configure VLAN 20 and VLAN 30 each with an SVI to which an IP address is assigned, packets can be sent from Host A to Host B directly through the Catalyst 3550 switch with no need for an external router ([Figure 7-2](#)).

Using the Interface Command

The Catalyst 3550 switch supports these interface types:

- Physical ports—including switch ports and routed ports
- VLANs—Switch Virtual Interface
- Port-channels—EtherChannel of interfaces

You can also configure a range of interfaces (see the “[Configuring a Range of Interfaces](#)” section on page 7-9).

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

- Type—Gigabit Ethernet (gigabitethernet or gi)
- Slot—The slot number on the switch. On the Catalyst 3550 switch, the slot number is 0.
- Port number—The interface number on the switch. The port numbers always begin at 1, starting at the left when facing the front of the switch, for example, **gigabitethernet 0/1**, **gigabitethernet 0/2**.

You can identify physical interfaces by physically checking the interface location on the switch. You can also use the IOS **show** 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.

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 and the number of the connector. In this example, Gigabit Ethernet interface 0/1 is selected:

```
Switch(config)# interface gigabitethernet0/1  
Switch(config-if)#
```



Note

You do not need to add a space between the interface type and interface number. For example, in the preceding line, you can specify either **gigabitethernet 0/1**, **gigabitethernet0/1**, **gi 0/1**, or **gi0/1**.

Step 3 Follow each interface command with the interface configuration commands your particular interface requires. The commands 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** 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 Layer 2 Interface”](#) section on page 7-16.

Enter the **show interfaces** privileged EXEC command to see a list of all interfaces installed in or configured for the switch. A report is provided for each interface that the device supports or for the specified interface:

```
Switch# show interfaces
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 0002.4b29.4400 (bia 0002.4b29.4400)
  Internet address is 172.20.135.204/27
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 10 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    67289 packets input, 6729152 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    97112 packets output, 14707453 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0002.4b29.4401 (bia 0002.4b29.4401)
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    215636 packets input, 22332831 bytes, 0 no buffer
    Received 85670 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    177366 packets output, 29241550 bytes, 0 underruns
    0 output errors, 2 collisions, 2 interface resets
    0 babbles, 0 late collision, 15 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

<output truncated>
```

Configuring a Range of Interfaces

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

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface range { <i>port-range</i> macro <i>macro_name</i> }	Enter interface configuration mode, and enter the range of interfaces (VLANs or physical ports) to be configured. <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 7-11. Each comma-separated <i>port-range</i> must consist of the same port type. You do not need to enter spaces before or after the comma. When you define a range, the space between the first port and the hyphen is required.
Step 3		You can now use the normal configuration commands to apply the configuration parameters to all interfaces in the range.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

- Valid entries for *port-range*:
 - vlan** *vlan-ID* - *vlan-ID*
 - gigabitethernet** slot/{*first port*} - {*last port*}, where slot is 0
 - port-channel** *port-channel-number* - *port-channel-number*, where *port-channel-number* is from 1 to 64
- You must add a space between the interface numbers and the hyphen when using the **interface range** command. For example, the command **interface range gigabitethernet 0/1 - 5** is a valid range; the command **interface range gigabitethernet 0/1-5** is not a valid range.
- The **interface range** command works only with VLAN interfaces that have been configured with the **interface vlan** command (the **show running-configuration** command displays the configured VLAN interfaces). VLAN interfaces not displayed by the **show running-configuration** command cannot be used with the **interface range** command.
- All interfaces in a range must be the same type; that is, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs.

This example shows how to use the **interface range** command to reenable Gigabit Ethernet interfaces 0/1 to 0/5:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 - 5
Switch(config-if)# no shutdown
Switch(config-if)#
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface GigabitEthernet0/4, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface GigabitEthernet0/5, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/5,
changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3,
changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/4,
changed state to up
```

This example shows how to use a comma to add different interface type strings to the range to reenable all Gigabit Ethernet interfaces in the range 0/1 to 0/3 and both Gigabit Ethernet interfaces 0/7 and 0/8:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 - 3, gigabitethernet0/7 - 8
Switch(config-if)# no shutdown
Switch(config-if)#
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet0/7, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet0/8, changed state to up
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/ 7,
changed state to up
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/ 2,
changed state to up
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/ 4,
changed state to up
```

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 together 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** command string, you must define the macro.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	define interface-range <i>macro_name</i> <i>interface-range</i>	Define the interface-range macro, and save it in NVRAM. <ul style="list-style-type: none"> The <i>macro_name</i> is a 32-character maximum character string. A macro can contain up to five comma-separated interface ranges. You do not need to enter spaces before or after the comma. Each <i>interface-range</i> must consist of the same port type.
Step 3	show running-config	Show the defined interface range macro configuration.
Step 4	interface range macro <i>macro_name</i>	Select the interface range to be configured using the values saved in the interface-range macro called <i>macro_name</i> . You can now use the normal configuration commands to apply the configuration to all in the macro range.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

- Valid entries for *interface-range*:
 - vlan** *vlan-ID* - *vlan-ID*
 - gigabitethernet** *slot*/*{first port}* - *{last port}*, where *slot* is 0
 - port-channel** *port-channel-number* - *port-channel-number*, where *port-channel-number* is from 1 to 64.
- You must add a space between the interface numbers and the hyphen when entering an *interface-range*. For example, **gigabitethernet 0/1 - 5** is a valid range; **gigabitethernet 0/1-5** is not a valid range.
- The VLAN interfaces must have been configured with the **interface vlan** command (the **show running-configuration** command displays the configured VLAN interfaces). VLAN interfaces not displayed by the **show running-configuration** command cannot be used as *interface-ranges*.
- All interfaces in a range must be the same type; that is, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs, but you can combine multiple interface types in a macro.

This example shows how to define an interface-range macro named `enet_list` to select Gigabit Ethernet interfaces 0/1 through 0/4:

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet0/1 - 4
Switch# end
```

This example shows how to display the defined interface-range macro named **enet_list**:

```
Switch# show running-config | include define
define interface-range enet_list GigabitEthernet0/1 - 4
Switch#
```

This example shows how to change to the interface configuration mode using the interface-range macro **enet_list**:

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

Configuring Layer 2 Interfaces

These sections describe the default interface configuration and the optional features that you can configure on most physical interfaces:

- [Default Layer 2 Ethernet Interface Configuration, page 7-12](#)
- [Configuring Interface Speed and Duplex Mode, page 7-13](#)
- [Configuring IEEE 802.3X Flow Control, page 7-15](#)
- [Adding a Description for an Interface, page 7-16](#)



Caution

If the interface is in Layer 3 mode, after entering interface configuration mode, you must enter the **switchport** command without any parameters to put the interface into Layer 2 mode. This shuts the interface down and then reenables it, which might generate messages on the device to which the interface is connected. In addition, when you use this command to put the interface into Layer 2 mode, you are deleting any Layer 3 characteristics configured on the interface.

Default Layer 2 Ethernet Interface Configuration

Table 7-1 shows the Layer 2 Ethernet interface default configuration. For more details on the VLAN parameters listed in the table, see [Chapter 8, “Creating and Maintaining VLANs.”](#) For details on controlling traffic to the port, see [Chapter 11, “Configuring Traffic Suppression and Traffic Control.”](#)

Table 7-1 Default Layer 2 Ethernet Interface Configuration

Feature	Default Setting
Operating mode	Layer 2 or switching mode (switchport command). Note Routing mode (no switchport command) is only an option when the enhanced multilayer switch image is installed.
Allowed VLAN range	VLANs 1 – 1005.
Default VLAN (for access ports)	VLAN 1.
Native VLAN (for 802.1Q trunks)	VLAN 1.
VLAN trunking	Switchport mode dynamic desirable (supports DTP).
Port enable state	All ports are enabled.
Port description	None defined.

Table 7-1 Default Layer 2 Ethernet Interface Configuration (continued)

Feature	Default Setting
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
Flow control	Flow control set to <i>off</i> for receive and <i>desired</i> for send.
EtherChannel (PAgP)	Disabled on all Ethernet ports. See Chapter 19, “Configuring EtherChannel.”
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked). Refer to the “Configuring Port Blocking” section on page 11-7.
Traffic suppression (broadcast, multicast, and unicast traffic)	Disabled. Refer to the “Configuring Traffic Suppression” section on page 11-2.
Protected port	Disabled. Refer to the “Configuring Protected Ports” section on page 11-6.
Port Fast	Disabled.

Configuring Interface Speed and Duplex Mode

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

- [Configuration Guidelines, page 7-13](#)
- [Setting the Interface Speed and Duplex Parameters, page 7-14](#)

Configuration Guidelines

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

- If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings.
- 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.



Note

GigaStack-to-GigaStack cascade connections operate in half-duplex mode, and GigaStack-to-GigaStack point-to-point connections operate in full-duplex mode.



Caution

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

Setting the Interface Speed and Duplex Parameters

You can configure interface speed on Gigabit Ethernet (10/100/1000-Mbps) interfaces; you cannot configure speed on Gigabit Interface Converter (GBIC) interfaces. You can configure duplex mode on any Gigabit Ethernet interfaces that are not set to autonegotiate. Because collisions are a major bottleneck in Ethernet networks, an effective solution is full-duplex communication. Normally, 10 Mbps ports operate in half-duplex mode, which means that stations can either receive or transmit. In full-duplex mode, two stations can transmit and receive at the same time. When packets can flow in both directions simultaneously, effective Ethernet bandwidth doubles to 20 Mbps for 10-Mbps interfaces, to 200 Mbps for Fast Ethernet interfaces, and to 2 Gbps for Gigabit interfaces.



Note

You cannot configure speed on GBIC ports. In addition, when a GBIC is inserted into a GBIC port, any preconfigured duplex value is ignored. If the GBIC is later removed, the preconfigured duplex value is restored.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter physical interface identification.
Step 3	speed [10 100 auto]	Enter the appropriate speed parameter for the interface or enter auto . Use the auto keyword to configure 1000 Mbps.
Step 4	duplex [auto full half]	Enter the duplex parameter for the interface.
Step 5	end	Return to privileged EXEC mode.
Step 6	show interface <i>interface-id</i>	Display the interface speed and duplex mode configuration.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to set the interface speed to 100 Mbps and the duplex mode to full on Gigabit Ethernet interface 0/4:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# speed 100
Switch(config-if)# duplex full
```

This example shows how to display the interface speed and duplex mode, as well as other characteristics, of Gigabit Ethernet interface 0/2:

```
Switch# show interface gigabitethernet0/2
GigabitEthernet0/2 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0002.4b29.4400 (bia 0002.4b29.4400)
  Internet address is 192.20.135.21/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:00, output hang never
```

```

Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  89245 packets input, 8451658 bytes, 0 no buffer
  Received 81551 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 input packets with dribble condition detected
60387 packets output, 5984015 bytes, 0 underruns
  0 output errors, 0 collisions, 16 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out

```

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 to stop transmitting until the condition clears. When the local device detects any congestion at its end, it can notify the link partner or the remote device of the congestion by transmitting a pause frame. On receiving a pause frame, the remote device stops transmitting any data packets. This prevents any loss of data packets during the congestion period.

Flow control can be implemented in two forms, symmetric and asymmetric. The symmetric implementation is useful for point-to-point links, and asymmetric is suitable for a hub-to-end node connections, where it is desirable for the hub to pause the end system, but not vice-versa. You use the **flowcontrol** interface configuration command to set the interface's ability to **receive** and **send** pause frames to **on**, **off**, or **desired**.

These rules apply to flow control settings on the device:

- **receive on** and **send on**: Flow control operates in both directions; pause frames can be sent by both the local device and the remote device to show link congestion.
- **receive on** and **send desired**: The port can receive pause frames and is able to send pause frames if the attached device supports flow control.
- **receive on** and **send off**: The port cannot send out pause frames, but can operate with an attached device that is required to or is able to send pause frames; the port is able to receive pause frames.
- **receive off** and **send on**: The port sends pause frames if the remote device supports flow control, but cannot receive pause frames from the remote device.
- **receive off** and **send desired**: The port cannot receive pause frames, but can send pause frames if the attached device supports flow control.
- **receive off** and **send off**: Flow control does not operate in either direction. In case of congestion, no indication will be given to the link partner and no pause frames will be transmitted or received by either device.



Note

For details on the command settings and the resulting flow control resolution on local and remote ports, refer to the **flowcontrol** command in the *Catalyst 3550 Multilayer Switch Command Reference* for this release.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the physical interface to be configured.
Step 3	flowcontrol { receive send } { on off desired }	Configure the flow control mode for the port.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interface <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** and **flowcontrol send off** interface configuration commands.

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 commands: **show configuration**, **show running-config**, and **show interfaces**.

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

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

This example shows how to add a description on Gigabit Ethernet interface 0/5:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/5
Switch(config-if)# description Channel-group to "Marketing"
```

Monitoring and Maintaining the Layer 2 Interface

You can perform the tasks in these sections to monitor and maintain the interfaces:

- [Monitoring Interface and Controller Status, page 7-17](#)
- [Clearing and Resetting the Interface Counters, page 7-19](#)
- [Shutting Down and Restarting the Interface, page 7-19](#)

Monitoring Interface and Controller Status

Commands entered at the privileged EXEC prompt display information about the interface, including the version of the software and the hardware, the controller status, and statistics about the interfaces. Table 7-2 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 for Release 12.1*.

Table 7-2 Show Commands for Interfaces

Command	Purpose
show interfaces [interface-id]	Display the status and configuration of all or a specific interface.
show interface interface-id status [err-disabled]	Display interface status or a list of interfaces in error-disabled state.
show interfaces [interface-id] switchport	Display administrative and operational status of switching (nonrouting) ports. You can use this command to determine if a port is in routing or switching mode.
show running config	Display the running configuration in RAM.
show version	Display the hardware configuration, software version, the names and sources of configuration files, and the boot images.

This example shows how to display the status and configuration of Gigabit Ethernet interface 0/2:

```
Switch# show interface gigabitethernet0/2
GigabitEthernet0/2 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0002.4b29.4400 (bia 0002.4b29.4400)
  Internet address is 192.20.135.21/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    89245 packets input, 8451658 bytes, 0 no buffer
    Received 81551 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    60387 packets output, 5984015 bytes, 0 underruns
    0 output errors, 0 collisions, 16 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

This example shows how to display the status of all interfaces:

```
Switch# show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi0/1	CubeA	connected	1	a-full	a-100	10/100/1000BaseTX
Gi0/2	CubeE	notconnect	1	auto	auto	10/100/1000BaseTX
Gi0/3	CubeF	disabled	1	auto	auto	10/100/1000BaseTX
Gi0/4	CubeG	notconnect	1	auto	auto	10/100/1000BaseTX
Gi0/5	CubeH	notconnect	routed	auto	auto	10/100/1000BaseTX
Gi0/6	CubeI	notconnect	routed	auto	auto	10/100/1000BaseTX
Gi0/7	CubeJ	connected	1	a-full	a-100	10/100/1000BaseTX
Gi0/8	CubeK	notconnect	1	auto	auto	10/100/1000BaseTX
Gi0/9	CubeL	disabled	1	auto	auto	10/100/1000BaseTX
Gi0/10	CubeB	notconnect	routed	auto	auto	10/100/1000BaseTX
Gi0/11	CubeC	notconnect	1	auto	auto	unknown
Gi0/12	CubeD	notconnect	1	auto	auto	unknown

This example shows how to display the status of switching ports:

```
Switch# show interfaces switchport
```

```
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

```
Port Protected: On
Unknown Unicast Traffic: Allowed
Unknown Multicast Traffic: Allowed
```

```
Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
```

```
Name: Gi0/2
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

```
Port Protected: On
Unknown Unicast Traffic: Allowed
Unknown Multicast Traffic: Allowed
```

```
Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
```

```
<output truncated>
```

Clearing and Resetting the Interface Counters

To clear the interface counters shown with the **show interfaces** command, use this EXEC command:

Command	Purpose
clear counters [<i>interface-id</i>]	Clear interface counters.

This example shows how to clear and reset the counters on Gigabit Ethernet interface 0/5:

```
Switch# clear counters gigabitethernet0/5
Clear "show interface" counters on this interface [confirm] y
Switch#
*Sep 30 08:42:55: %CLEAR-5-COUNTERS: Clear counter on interface GigabitEthernet0/5
by vty1 (171.69.115.10)
```

The **clear counters** command clears all current interface counters from the interface unless optional arguments are specified to clear only a specific interface type from a specific interface number.



Note

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

To clear and reset interfaces, perform this task (under normal circumstances, you do not need to clear the hardware logic on interfaces):

	Command	Purpose
Step 1	clear interface <i>interface-id</i>	Reset the hardware logic on an interface.
Step 2	clear line [<i>number</i> console 0 vty number]	Reset the hardware logic on an asynchronous serial line.

This example shows how to clear and reset Gigabit Ethernet interface 0/5:

```
Switch# clear interface gigabitethernet0/5
```

Shutting Down and Restarting the Interface

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

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

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

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

This example shows how to shut down Gigabit Ethernet interface 0/5:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/5
Switch(config-if)# shutdown
Switch(config-if)#
*Sep 30 08:33:47: %LINK-5-CHANGED: Interface GigabitEthernet0/5, changed state to a
administratively down
```

This example shows how to reenable Gigabit Ethernet interface 0/5:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/5
Switch(config-if)# no shutdown
Switch(config-if)#
*Sep 30 08:36:00: %LINK-3-UPDOWN: Interface GigabitEthernet0/5, changed state to up
```

To verify that an interface is disabled, enter the **show interfaces** privileged EXEC command. An interface that has been shut down is shown as *administratively down* in the **show interfaces** command display as with Gigabit Ethernet interface 0/1 in this example.

```
Switch# show interfaces
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 0002.4b29.4400 (bia 0002.4b29.4400)
  Internet address is 172.20.135.204/27
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 10 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    67713 packets input, 6765900 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    97420 packets output, 14725933 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0002.4b29.4401 (bia 0002.4b29.4401)
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    217042 packets input, 22469265 bytes, 0 no buffer
    Received 86049 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    177863 packets output, 29278781 bytes, 0 underruns
    0 output errors, 2 collisions, 2 interface resets
```

```

    0 babbles, 0 late collision, 15 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/2 is administratively down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0002.4b29.4403 (bia 0002.4b29.4403)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed

<output truncated>

```

Configuring Layer 3 Interfaces

The Catalyst 3550 with the enhanced multilayer switch image supports three types of Layer 3 interfaces for routing and bridging:

- **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.

For information about assigning Layer 2 ports to VLANs, see [Chapter 8, “Creating and Maintaining VLANs.”](#)

- **Layer 3 EtherChannel ports:** EtherChannel interfaces made up of routed ports. EtherChannel port interfaces are described in [Chapter 19, “Configuring EtherChannel.”](#)
- **Routed ports:** Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** command.



Note

On a Catalyst 3550-12T switch, we recommend configuring a maximum of 16 routed interfaces (SVIs and routed ports) simultaneously to allow enough system resources to support features enabled on these interfaces. If requirements exceed the system hardware allocation, processing overflow is sent to the CPU, which degrades performance. Refer to the [“Optimizing System Resources for User-Selected Features”](#) section on page 6-41 for more information about feature combinations.

All Layer 3 interfaces require an IP address to route traffic. The following procedure shows how to configure an interface as a Layer 3 interface and how to assign an IP addresses 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. When you use this command to put the interface into Layer 3 mode, you are also deleting any Layer 2 characteristics configured on the interface.

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

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

This example shows how to configure Gigabit Ethernet interface 0/10 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 gigabitethernet0/10
Switch(config)# no switchport
Switch(config-if)# ip address 10.1.2.3 255.255.0.0
Switch(config-if)# no shutdown
Switch(config-if)# end
```

This example uses the **show interface** command to display the interface IP address configuration and status of Gigabit Ethernet interface 0/2:

```
Switch(config)# show interface gigabitethernet0/2
GigabitEthernet0/2 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0002.4b29.4400 (bia 0002.4b29.4400)
  Internet address is 192.20.135.21/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    89604 packets input, 8480109 bytes, 0 no buffer
    Received 81848 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    60665 packets output, 6029820 bytes, 0 underruns
    0 output errors, 0 collisions, 16 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

This example uses the **show ip interface** command to display the detailed configuration and status of the same interface, Gigabit Ethernet interface 0/2:

```
Switch# show ip interface gigabitethernet0/2
GigabitEthernet0/2 is up, line protocol is up
  Internet address is 192.20.135.21/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

This example uses the **show running-config** command to display the interface IP address configuration of Gigabit Ethernet interface 0/2:

```
Switch# show running-config interfaces gigabitethernet0/2
Building configuration...

Current configuration : 122 bytes
!
interface GigabitEthernet0/2
  no switchport
  ip address 192.20.135.21 255.255.255.0
  speed 100
  mls qos trust dscp
end
```

