



Configuring Layer 2 Ethernet Interfaces

This chapter describes how to use the command-line interface (CLI) to configure Fast Ethernet and Gigabit Ethernet interfaces for Layer 2 switching on the Catalyst 4000 family switches. It also provides guidelines, procedures, and configuration examples. The configuration tasks in this chapter apply to Fast Ethernet and Gigabit Ethernet interfaces on any module, including the uplink ports on the supervisor engine.

This chapter consists of the following sections:

- [Layer 2 Switching Overview, page 6-1](#)
- [Layer 2 Interface Configuration Guidelines and Restrictions, page 6-4](#)
- [Default Layer 2 Ethernet Interface Configuration, page 6-5](#)
- [Configuring Ethernet Interfaces for Layer 2 Switching, page 6-5](#)



Note

To configure Layer 3 interfaces, see [Chapter 10, “Configuring Layer 3 Interfaces.”](#)



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference for the Catalyst 4006 Switch with Supervisor Engine III* and the publications at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

Layer 2 Switching Overview

The following sections describe how Layer 2 switching works on the Catalyst 4000 family switches:

- [Understanding Layer 2 Ethernet Switching, page 6-1](#)
- [Understanding VLAN Trunks, page 6-2](#)
- [Layer 2 Interface Modes, page 6-4](#)

Understanding Layer 2 Ethernet Switching

The Catalyst 4006 switch with Supervisor Engine III support simultaneous, parallel connections between Layer 2 Ethernet segments. Switched connections between Ethernet segments last only for the duration of the packet. New connections can be made between different segments for successive packets

The Catalyst 4006 switch with Supervisor Engine III solves congestion problems caused by high-bandwidth devices and a large number of users by assigning each device (for example, a server) to its own 10-, 100-, or 1000-Mbps segment. Because each Ethernet interface on the switch represents a separate Ethernet segment, servers in a properly configured switched environment achieve full access to the bandwidth.

Because collisions are a major bottleneck in Ethernet networks, an effective solution is full-duplex communication. Normally, Ethernet operates in half duplex mode, which means that stations can either receive or transmit. In full duplex mode, two devices 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 and to 200 Mbps for Fast Ethernet interfaces. Gigabit Ethernet interfaces on the Catalyst 4006 switch with Supervisor Engine III are full-duplex mode only, providing 2-Gbps effective bandwidth.

Switching Frames Between Segments

Each Ethernet interface on a Catalyst 4000 family switch can connect to a single workstation or server, or to a hub through which workstations or servers connect to the network.

On a typical Ethernet hub, all ports connect to a common backplane within the hub, and the bandwidth of the network is shared by all devices attached to the hub. If two devices establish a session that uses a significant level of bandwidth, the network performance of all other stations attached to the hub is degraded.

To reduce degradation, the switch treats each interface as an individual segment. When stations on different interfaces need to communicate, the switch forwards frames from one interface to the other at wire speed to ensure that each session receives full bandwidth.

To switch frames between interfaces efficiently, the switch maintains an address table. When a frame enters the switch, it associates the MAC address of the sending station with the interface on which it was received.

Building the MAC Address Table

The Catalyst 4006 switch with Supervisor Engine III builds the MAC address table by using the source address of the frames received. When the switch receives a frame for a destination address not listed in its MAC address table, it floods the frame to all interfaces of the same VLAN except the interface that received the frame. When the destination device replies, the switch adds its relevant source address and interface ID to the address table. The switch then forwards subsequent frames to a single interface without flooding to all interfaces.

The address table can store at least 32,000 address entries without flooding any entries. The switch uses an aging mechanism, defined by a configurable aging timer, so if an address remains inactive for a specified number of seconds, it is removed from the address table.

Understanding VLAN Trunks

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network.

Two trunking encapsulations are available on all Ethernet interfaces:

- Inter-Switch Link (ISL)—ISL is a Cisco-proprietary trunking encapsulation.



Note Blocking Gigabit ports on the WS-X4418-GB and WS-X4412-2GB-T modules do not support ISL. Ports 3 - 18 are blocking Gigabit ports on the WS-X4418-GB module. Ports 1 - 12 are blocking Gigabit ports on the WS-X4412-2GB-T module.

- 802.1Q—802.1Q is an industry-standard trunking encapsulation.

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannel, see [Chapter 11, “Understanding and Configuring EtherChannel.”](#)

Ethernet trunk interfaces support different trunking modes (see [Table 6-2 on page 6-4](#)). You can specify whether the trunk uses ISL encapsulation, 802.1Q encapsulation, or if the encapsulation type is autonegotiated.

To autonegotiate trunking, the interfaces must be in the same VTP domain. Use the **trunk** or **nonegotiate** keywords to force interfaces in different domains to trunk. For more information on VTP domains, see [Chapter 9, “Understanding and Configuring VTP.”](#)

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP). DTP supports autonegotiation of both ISL and 802.1Q trunks.

Encapsulation Types

[Table 6-1](#) lists the Ethernet trunk encapsulation types.

Table 6-1 Ethernet Trunk Encapsulation Types

Encapsulation Type	Encapsulation Command	Function
ISL	switchport trunk encapsulation isl	Specifies ISL encapsulation on the trunk link.
802.1Q	switchport trunk encapsulation dot1q	Specifies 802.1Q encapsulation on the trunk link.
Negotiate	switchport trunk encapsulation negotiate	Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface.

The trunking mode, the trunk encapsulation type, and the hardware capabilities of the two connected interfaces determine whether a link becomes an ISL or 802.1Q trunk.

Layer 2 Interface Modes

Table 6-2 lists the Layer 2 interface modes and describes how they function on Ethernet interfaces.

Table 6-2 Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not change.
switchport mode dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk , desirable , or auto mode.
switchport mode dynamic auto	Makes the interface convert the link to a trunk link if the neighboring interface is set to trunk or desirable mode. This is the default mode for all Ethernet interfaces.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not change.
switchport nonegotiate	Puts the interface into permanent trunking mode but prevents the interface from generating DTP frames. You must configure the neighboring interface manually as a trunk interface to establish a trunk link.



Note

DTP is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly. To avoid this problem, ensure that interfaces connected to devices that do not support DTP are configured with the **access** keyword if you do not intend to trunk across those links. To enable trunking to a device that does not support DTP, use the **nonegotiate** keyword to cause the interface to become a trunk without generating DTP frames.

Layer 2 Interface Configuration Guidelines and Restrictions

The following guidelines and restrictions apply when configuring Layer 2 interfaces:

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. Non-Cisco 802.1Q switches maintain only one instance of spanning tree for all VLANs allowed on the trunks.

When you connect a Cisco switch to a non-Cisco device through an 802.1Q trunk, the Cisco switch combines the spanning tree instance of the native VLAN of the trunk with the spanning tree instance of the non-Cisco 802.1Q switch. However, spanning tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

- Ensure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the VLAN on one end of the trunk is different from the VLAN on the other end, spanning tree loops might result.

- Disabling spanning tree on any VLAN of an 802.1Q trunk can potentially cause spanning tree loops.

Default Layer 2 Ethernet Interface Configuration

Table 6-3 shows the Layer 2 Ethernet interface default configuration.

Table 6-3 Layer 2 Ethernet Interface Default Configuration

Feature	Default Value
Interface mode	switchport mode dynamic auto
Trunk encapsulation	switchport trunk encapsulation negotiate
Allowed VLAN range	VLANs 1–1005
VLAN range eligible for pruning	VLANs 2–1001
Default VLAN (for access ports)	VLAN 1
Native VLAN (for 802.1Q only trunks)	VLAN 1
Spanning Tree Protocol (STP)	Enabled for all VLANs
STP port priority	128
STP port cost	<ul style="list-style-type: none"> • 19 for 10/100-Mbps Fast Ethernet interfaces • 19 for 100-Mbps Fast Ethernet interfaces • 4 for 1000-Mbps Gigabit Ethernet interfaces

Configuring Ethernet Interfaces for Layer 2 Switching

The following sections describe how to configure Layer 2 switching on the Catalyst 4006 switch with Supervisor Engine III:

- [Configuring an Ethernet Interface as a Layer 2 Trunk, page 6-5](#)
- [Configuring an Interface as a Layer 2 Access Port, page 6-7](#)
- [Clearing Layer 2 Configuration, page 6-9](#)

Configuring an Ethernet Interface as a Layer 2 Trunk



Note

The default for Layer 2 interfaces is **switchport mode dynamic auto**. If the neighboring interface supports trunking and is configured to trunk mode or dynamic desirable mode, the link becomes a Layer 2 trunk. By default, trunks negotiate encapsulation. If the neighboring interface supports ISL and 802.1Q encapsulation and both interfaces are set to negotiate the encapsulation type, the trunk uses ISL encapsulation.

To configure an interface as a Layer 2 trunk, perform this task:

Task	Command
Step 1 Select the interface to configure.	Switch(config)# interface {fastethernet gigabitethernet} slot/port
Step 2 (Optional) Shut down the interface to prevent traffic flow until configuration is complete.	Switch(config-if)# shutdown
Step 3 (Optional) Specify the encapsulation. Note You must enter this command with either the isl or dot1q keyword to support the switchport mode trunk command, which is not supported by the default mode (negotiate).	Switch(config-if)# switchport trunk encapsulation {isl dot1q negotiate}
Step 4 Configure the interface as a Layer 2 trunk. (Required only if the interface is a Layer 2 access port or to specify the trunking mode.)	Switch(config-if)# switchport mode {dynamic {auto desirable} trunk}
Step 5 (Optional) Specify the access VLAN, which is used if the interface stops trunking. The access VLAN is not used as the native VLAN.	Switch(config-if)# switchport access vlan vlan_num
Step 6 For 802.1Q trunks, specify the native VLAN. Note If you do not set the native VLAN, then the default is used (VLAN 1).	Switch(config-if)# switchport trunk native vlan vlan_num
Step 7 (Optional) Configure the list of VLANs allowed on the trunk. All VLANs are allowed by default. You cannot remove any of the default VLANs from a trunk.	Switch(config-if)# switchport trunk allowed vlan {add except all remove} vlan ¹ [,vlan[,vlan[,...]]]
Step 8 (Optional) Configure the list of VLANs allowed to be pruned from the trunk (see the “ Understanding VTP Pruning ” section on page 9-4). The default list of VLANs allowed to be pruned contains all VLANs, except for VLAN 1.	Switch(config-if)# switchport trunk pruning vlan {add except except none remove} vlan ¹ [,vlan[,vlan[,...]]]
Step 9 Activate the interface. (Required only if you shut down the interface.)	Switch(config-if)# no shutdown
Step 10 Exit configuration mode.	Switch(config-if)# end
Step 11 Display the running configuration of the interface.	Switch# show running-config interface {fastethernet gigabitethernet} slot/port
Step 12 Display the switch port configuration of the interface.	Switch# show interfaces [fastethernet gigabitethernet] slot/port switchport
Step 13 Display the trunk configuration of the interface.	Switch# show interfaces [{fastethernet gigabitethernet} slot/port] trunk

1. The *vlan* parameter is either a single VLAN number from 1 to 1005 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated *vlan* parameters or in dash-specified ranges.

This example shows how to configure the Fast Ethernet interface 5/8 as an 802.1Q trunk. This example assumes that the neighbor interface is configured to support 802.1Q trunking and that the native VLAN defaults to VLAN 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/8
Switch(config-if)# shutdown
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport trunk encapsulation dot1q
```

```
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# exit
```

This example shows how to verify the configuration:

```
Switch# show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
  switchport mode dynamic desirable
  switchport trunk encapsulation dot1q
end
```

```
Switch# show interfaces fastethernet 5/8 switchport
Name: Fa5/8
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Enabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

```
Switch# show interfaces fastethernet 5/8 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa5/8	desirable	n-802.1q	trunking	1

```
Port      Vlans allowed on trunk
Fa5/8 1-1005
```

```
Port      Vlans allowed and active in management domain
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005
```

```
Switch#
```

Configuring an Interface as a Layer 2 Access Port



Note

If you assign an interface to a VLAN that does not exist, the interface is not operational until you create the VLAN in the VLAN database (see the [“Configuring VLANs in Global Mode”](#) section on page 7-6).

To configure an interface as a Layer 2 access port, perform this task:

Task	Command
Step 1 Select the interface to configure.	Switch(config)# interface { fastethernet gigabitethernet } <i>slot/port</i>
Step 2 (Optional) Shut down the interface to prevent traffic flow until configuration is complete.	Switch(config-if)# shutdown
Step 3 Configure the interface for Layer 2 switching: <ul style="list-style-type: none"> You must enter the switchport command once without any keywords to configure the interface as a Layer 2 port before you can enter additional switchport commands with keywords. Required only if you previously entered the no switchport command for the interface. 	Switch(config-if)# switchport
Step 4 Configure the interface as a Layer 2 access port.	Switch(config-if)# switchport mode access
Step 5 Place the interface in a VLAN.	Switch(config-if)# switchport access vlan <i>vlan_num</i>
Step 6 Activate the interface. (Required only if you shut down the interface.)	Switch(config-if)# no shutdown
Step 7 Exit configuration mode.	Switch(config-if)# end
Step 8 Display the running configuration of the interface.	Switch# show running-config interface { fastethernet gigabitethernet } <i>slot/port</i>
Step 9 Display the switch port configuration of the interface.	Switch# show interfaces [{ fastethernet gigabitethernet } <i>slot/port</i>] switchport

This example shows how to configure the Fast Ethernet interface 5/6 as an access port in VLAN 200:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/6
Switch(config-if)# shutdown
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 200
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# exit
```

This example shows how to verify the configuration:

```
Switch# show running-config interface fastethernet 4/1
Building configuration...
!
Current configuration :33 bytes
interface FastEthernet4/1
  switchport access vlan 200
  switchport mode access
end

Switch# show running-config interface fastethernet 4/1 switchport
Name:Fa4/1
Switchport:Enabled
Administrative Mode:dynamic auto
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)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Switch#

```

Clearing Layer 2 Configuration

To clear Layer 2 configuration on an interface, perform this task:

	Task	Command
Step 1	Select the interface to configure.	Switch(config)# default interface { fastethernet gigabitethernet } <i>slot/port</i>
Step 2	Exit configuration mode.	Switch(config-if)# end
Step 3	Display the running configuration of the interface.	Switch# show running-config interface { fastethernet gigabitethernet } <i>slot/port</i>
Step 4	Display the switch port configuration of the interface.	Switch# show interfaces [{ fastethernet gigabitethernet } <i>slot/port</i>] switchport

This example shows how to disable Layer 2 configuration on the Fast Ethernet interface 5/6:

```

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# default interface fastethernet 5/6
Switch(config)# end
Switch# exit

```

This example shows how to verify the configuration:

```

Switch# show running-config interface fastethernet 5/6
Building configuration...
Current configuration:
!
interface FastEthernet5/6
end

Switch# show interfaces fastethernet 5/6 switchport
Name: Fa5/6
Switchport: Enabled
Switch#

```

