CHAPTER 13

Configuring LAN Ports for Layer 2 Switching

This chapter describes how to use the command-line interface (CLI) to configure Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet LAN ports for Layer 2 switching in Cisco IOS Software Release 12.2SX. The configuration tasks in this chapter apply to LAN ports on switching modules and to the LAN ports on the supervisor engine and Cisco ME 6500 Series Ethernet switches.

Note

- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Software Releases 12.2SX Command References at this URL:

  http://www.cisco.com/en/US/docs/ios/mcl/122sx_mcl.html

- To configure Layer 3 interfaces, see Chapter 24, "Configuring Layer 3 Interfaces."

This chapter consists of these sections:

- Understanding Layer 2 Switching, page 13-1
- Default Layer 2 LAN Interface Configuration, page 13-5
- Layer 2 LAN Interface Configuration Guidelines and Restrictions, page 13-5
- Configuring LAN Interfaces for Layer 2 Switching, page 13-6

Understanding Layer 2 Switching

These sections describe how Layer 2 switching works in Cisco IOS Software Release 12.2SX:

- Understanding Layer 2 Ethernet Switching, page 13-1
- Understanding VLAN Trunks, page 13-3
- Layer 2 LAN Port Modes, page 13-4

Understanding Layer 2 Ethernet Switching

These sections describe Layer 2 Ethernet switching:

- Layer 2 Ethernet Switching Overview, page 13-2
- Switching Frames Between Segments, page 13-2
- Building the Address Table, page 13-2

Layer 2 Ethernet Switching Overview

Layer 2 Ethernet ports on Cisco switches 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 the next packet.

Cisco switches that support Layer 2 Ethernet ports solve congestion problems caused by high-bandwidth devices and by a large number of users by assigning each device (for example, a server) to its own 10-, 100-, or 1000-Mbps collision domain. Because each LAN port connects to a separate Ethernet collision domain, servers in a properly configured switched environment achieve full access to the bandwidth.

Because collisions cause significant congestion 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 stations can transmit and receive at the same time. When packets can flow in both directions simultaneously, the effective Ethernet bandwidth doubles.

Switching Frames Between Segments

Each Layer 2 Ethernet port 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 stations 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 considers each LAN port to be an individual segment. When stations connected to different LAN ports need to communicate, the switch forwards frames from one LAN port to the other at wire speed to ensure that each session receives full bandwidth.

To switch frames between LAN ports efficiently, the switch maintains an address table. When a frame enters the switch, it associates the MAC address of the sending network device with the LAN port on which it was received.

Building the Address Table

The address table is built by using the source address of the frames received. When the switch receives a frame for a destination address not listed in its address table, it floods the frame to all LAN ports of the same VLAN except the port that received the frame. When the destination station replies, the switch adds its relevant source address and port ID to the address table. The switch then forwards subsequent frames to a single LAN port without flooding to all LAN ports.

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.

Notification of Address Table Changes

You can configure the switch to maintain a history of dynamic additions and removals of address table entries associated with a particular LAN port. The change history can be sent as an SNMP trap notification or it can be read manually from the SNMP MIB.

Understanding VLAN Trunks

These sections describe VLAN trunks in Cisco IOS Software Release 12.2SX:

- Trunking Overview, page 13-3
- Encapsulation Types, page 13-3

Trunking Overview

Note For information about VLANs, see Chapter 17, "Configuring VLANs."

A trunk is a point-to-point link between the switch and another networking device. 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 ports:

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

  Note The following switching modules do not support ISL encapsulation:

  • WS-X6502-10GE
  • WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF
  • WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF

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

You can configure a trunk on a single Ethernet port or on an EtherChannel. For more information about EtherChannel, see Chapter 15, "Configuring EtherChannels."

Ethernet trunk ports support several trunking modes (see Table 13-2 on page 13-4). You can specify whether the trunk uses ISL or 802.1Q encapsulation, and if the encapsulation type is autonegotiated.

Note You can configure LAN ports to negotiate the encapsulation type. You cannot configure WAN interfaces to negotiate the encapsulation type.

The Dynamic Trunking Protocol (DTP) manages trunk autonegotiation on LAN ports. DTP supports autonegotiation of both ISL and 802.1Q trunks.

To autonegotiate trunking, the LAN ports must be in the same VTP domain. Use the **trunk** or **nonegotiate** keywords to force LAN ports in different domains to trunk. For more information on VTP domains, see Chapter 16, "Configuring VTP."

Encapsulation Types

Table 13-1 lists the Ethernet trunk encapsulation types.

Table 13-1 Ethernet Trunk Encapsulation Types

Encapsulation	Function
switchport trunk encapsulation isl	Specifies ISL encapsulation on the trunk link. **Note** Some modules do not support ISL encapsulation (see the "Trunking Overview" section on page 13-3).
switchport trunk encapsulation dot1q	Specifies 802.1Q encapsulation on the trunk link.
switchport trunk encapsulation negotiate	Specifies that the LAN port negotiate with the neighboring LAN port to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring LAN port.

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

Layer 2 LAN Port Modes

Table 13-2 lists the Layer 2 LAN port modes and describes how they function on LAN ports.

Table 13-2 Layer 2 LAN Port Modes

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

Default Layer 2 LAN Interface Configuration

Table 13-3 shows the Layer 2 LAN port default configuration.

Table 13-3 Layer 2 LAN Interface Default Configuration

Feature	Default
Interface mode:	
• Before entering the **switchport** command	Layer 3 (unconfigured)
• After entering the **switchport** command	**switchport mode dynamic desirable**
Trunk encapsulation	**switchport trunk encapsulation negotiate**
Allowed VLAN range	VLANs 1 to 4094, except reserved VLANs (see Table 17-1 on page 17-2)
VLAN range eligible for pruning	VLANs 2 to 1001
Default access VLAN	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1
Spanning Tree Protocol (STP)	Enabled for all VLANs
STP port priority	128
STP port cost	• 100 for 10-Mbps Ethernet LAN ports • 19 for 10/100-Mbps Fast Ethernet LAN ports • 19 for 100-Mbps Fast Ethernet LAN ports • 4 for 1,000-Mbps Gigabit Ethernet LAN ports • 2 for 10,000-Mbps 10-Gigabit Ethernet LAN ports

Layer 2 LAN Interface Configuration Guidelines and Restrictions

When configuring Layer 2 LAN ports, follow these guidelines and restrictions:

- The following switching modules do not support ISL encapsulation:
  - WS-X6502-10GE
  - WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF
  - WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF

- The following configuration guidelines and restrictions apply when using 802.1Q trunks and impose some limitations on the trunking strategy for a network. Note these restrictions when using 802.1Q trunks:
  - When connecting Cisco switches through an 802.1q trunk, make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops might result.
  - Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure your network is free of physical loops before disabling spanning tree.
  - When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Cisco Shared Spanning Tree (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
  - Non-Cisco 802.1Q switches maintain only a single instance of spanning tree (the Mono Spanning Tree, or MST) that defines the spanning tree topology for all VLANs. When you connect a Cisco switch to a non-Cisco switch through an 802.1Q trunk, the MST of the non-Cisco switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning tree topology known as the Common Spanning Tree (CST).
  - Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the non-Cisco 802.1q cloud receive these flooded BPDUs. This allows Cisco switches to maintain a per-VLAN spanning tree topology across a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single broadcast segment between all switches connected to the non-Cisco 802.1q cloud through 802.1q trunks.
  - Make certain that the native VLAN is the same on all of the 802.1q trunks connecting the Cisco switches to the non-Cisco 802.1q cloud.
  - If you are connecting multiple Cisco switches to a non-Cisco 802.1q cloud, all of the connections must be through 802.1q trunks. You cannot connect Cisco switches to a non-Cisco 802.1q cloud through ISL trunks or through access ports. Doing so causes the switch to place the ISL trunk port or access port into the spanning tree “port inconsistent” state and no traffic will pass through the port.

Configuring LAN Interfaces for Layer 2 Switching

These sections describe how to configure Layer 2 switching inCisco IOS Software Release 12.2SX :

Note Use the **default interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* command to revert an interface to its default configuration.

Configuring a LAN Port for Layer 2 Switching

To configure a LAN port for Layer 2 switching, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** *type*[1] *slot/port*	Selects the LAN port to configure.
Step 2	Router(config-if)# **shutdown**	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3	Router(config-if)# **switchport**	Configures the LAN port for Layer 2 switching. **Note** You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional **switchport** commands with keywords.
	Router(config-if)# **no switchport**	Clears Layer 2 LAN port configuration.
Step 4	Router(config-if)# **no shutdown**	Activates the interface. (Required only if you shut down the interface.)
Step 5	Router(config-if)# **end**	Exits configuration mode.
Step 6	Router# **show running-config interface** [*type*[1] *slot/port*]	Displays the running configuration of the interface.
Step 7	Router# **show interfaces** [*type*[1] *slot/port*] **switchport**	Displays the switch port configuration of the interface.
Step 8	Router# **show interfaces** [*type*[1] *slot/port*] **trunk**	Displays the trunk configuration of the interface.

[1] *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

After you enter the **switchport** command, the default mode is **switchport mode dynamic desirable**. If the neighboring port supports trunking and is configured to allow trunking, the link becomes a Layer 2 trunk when you enter the **switchport** command. By default, LAN trunk ports negotiate encapsulation. If the neighboring port supports ISL and 802.1Q encapsulation and both ports are set to negotiate the encapsulation type, the trunk uses ISL encapsulation (10-Gigabit Ethernet ports do not support ISL encapsulation).

Configuring MAC Address Table Notification

Note

- Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 13-7 before performing the tasks in this section.
- To send SNMP trap notifications using this feature, you must also enable the global MAC trap flag, using the **snmp-server enable mac-notification change** command.

With Release 12.2(33)SXH and later releases, to configure the MAC address table notification feature, perform this task:

	Command	Purpose
Step 1	`Router(config)# mac-address-table notification change [interval value] [history size]`	Enables sending notification of dynamic changes to MAC address table. (Optional) Sets the minimum change-sending interval in seconds. (Optional) Sets the number of entries in the history buffer.
	`Router(config)# no mac-address-table notification change`	Reverts to the default (no change information is sent).
Step 2	`Router(config)# interface type`[1] `slot/port`	Selects the LAN port to configure.
Step 3	`Router(config-if)# snmp trap mac-notification change [added | removed]`	For MAC addresses that are associated with this LAN port, enable SNMP trap notification when MAC addresses are added to or removed from the address table. (Optional) To notify only when a MAC address is added to the table, use the **added** option. To notify only when a MAC address is removed, use the **removed** option.
	`Router(config-if)# no snmp trap mac-notification change`	Disables SNMP trap notification of MAC address table changes associated with this LAN port.
Step 4	`Router(config-if)# end`	Exits interface configuration mode.
Step 5	`Router# show mac-address-table notification`	Displays whether this feature is enabled, the notification interval, and the history table maximum size. Displays history table contents.
Step 6	`Router# show mac-address-table notification [type slot/port]`	Displays the interface-specific flags for the specified interface. If slot and port are not specified, the flags for all interfaces will be displayed.

[1] *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When configuring the notification parameters, note the following information:

- The **interval** *value* parameter can be configured from 0 seconds (immediate) to 2,147,483,647 seconds. The default is 1 second.
- The **history** *size* parameter can be configured from 0 entries to 500 entries. The default is 1 entry.

This example shows how to configure the SNMP notification of dynamic additions to the MAC address table of addresses on the Fast Ethernet ports 5/7 and 5/8. Notifications of changes will be sent no more frequently than 5 seconds, and up to 25 changes can be stored and sent in that interval:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mac-address-table notification change interval 5 history 25
Router(config)# interface fastethernet 5/7
Router(config-if)# snmp trap mac-notification change added
Router(config-if)# end
Router(config)# interface fastethernet 5/8
Router(config-if)# snmp trap mac-notification change added
Router(config-if)# end
Router# exit
```

Configuring a Layer 2 Switching Port as a Trunk

These sections describe configuring a Layer 2 switching port as a trunk:

- Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk, page 13-9
- Configuring the Layer 2 Trunk to Use DTP, page 13-10
- Configuring the Layer 2 Trunk Not to Use DTP, page 13-10
- Configuring the Access VLAN, page 13-11
- Configuring the 802.1Q Native VLAN, page 13-11
- Configuring the List of VLANs Allowed on a Trunk, page 13-12
- Configuring the List of Prune-Eligible VLANs, page 13-13
- Completing Trunk Configuration, page 13-13
- Verifying Layer 2 Trunk Configuration, page 13-14
- Configuration and Verification Examples, page 13-14

Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk

Note

- Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 13-7 before performing the tasks in this section.
- When you enter the **switchport** command with no other keywords (Step 3 in the previous section), the default mode is **switchport mode dynamic desirable** and **switchport trunk encapsulation negotiate**.

To configure the Layer 2 switching port as an ISL or 802.1Q trunk, perform this task:

Command	Purpose
`Router(config-if)#` **`switchport trunk encapsulation {isl | dot1q | negotiate}`**	(Optional) Configures the encapsulation, which configures the Layer 2 switching port as either an ISL or 802.1Q trunk.
`Router(config-if)#` **`no switchport trunk encapsulation`**	Reverts to the default trunk encapsulation mode (**negotiate**).

When configuring the Layer 2 switching port as an ISL or 802.1Q trunk, note the following information:

- The **switchport mode trunk** command (see the "Configuring the Layer 2 Trunk Not to Use DTP" section on page 13-10) is not compatible with the **switchport trunk encapsulation negotiate** command.
- To support the **switchport mode trunk** command, you must configure the encapsulation as either ISL or 802.1Q.
- The following switching modules do not support ISL encapsulation:
  - WS-X6502-10GE
  - WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF
  - WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF

Note Complete the steps in the "Completing Trunk Configuration" section on page 13-13 after performing the tasks in this section.

Configuring the Layer 2 Trunk to Use DTP

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 13-7 before performing the tasks in this section.

To configure the Layer 2 trunk to use DTP, perform this task:

Command	Purpose
`Router(config-if)# switchport mode dynamic {auto | desirable}`	(Optional) Configures the trunk to use DTP.
`Router(config-if)# no switchport mode`	Reverts to the default trunk trunking mode (**switchport mode dynamic desirable**).

When configuring the Layer 2 trunk to use DTP, note the following information:

- Required only if the interface is a Layer 2 access port or to specify the trunking mode.
- See Table 13-2 on page 13-4 for information about trunking modes.

Note Complete the steps in the "Completing Trunk Configuration" section on page 13-13 after performing the tasks in this section.

Configuring the Layer 2 Trunk Not to Use DTP

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 13-7 before performing the tasks in this section.

To configure the Layer 2 trunk not to use DTP, perform this task:

	Command	Purpose
Step 1	`Router(config-if)# switchport mode trunk`	(Optional) Configures the port to trunk unconditionally.
	`Router(config-if)# no switchport mode`	Reverts to the default trunk trunking mode (**switchport mode dynamic desirable**).
Step 2	`Router(config-if)# switchport nonegotiate`	(Optional) Configures the trunk not to use DTP.
	`Router(config-if)# no switchport nonegotiate`	Enables DTP on the port.

When configuring the Layer 2 trunk not to use DTP, note the following information:

- Before entering the **switchport mode trunk** command, you must configure the encapsulation (see the "Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk" section on page 13-9).
- To support the **switchport nonegotiate** command, you must enter the **switchport mode trunk** command.
- Enter the **switchport mode dynamic trunk** command. See Table 13-2 on page 13-4 for information about trunking modes.
- Before entering the **switchport nonegotiate** command, you must configure the encapsulation (see the "Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk" section on page 13-9) and configure the port to trunk unconditionally with the **switchport mode trunk** command (see the "Configuring the Layer 2 Trunk to Use DTP" section on page 13-10).

Note Complete the steps in the "Completing Trunk Configuration" section on page 13-13 after performing the tasks in this section.

Configuring the Access VLAN

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 13-7 before performing the tasks in this section.

To configure the access VLAN, perform this task:

Command	Purpose
`Router(config-if)#` **`switchport access vlan`** *`vlan_ID`*	(Optional) Configures the access VLAN, which is used if the interface stops trunking. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 17-1 on page 17-2). **Note** If VLAN locking is enabled, enter the VLAN name instead of the VLAN number. For more information, see the "VLAN Locking" section on page 17-9.
`Router(config-if)#` **`no switchport access vlan`**	Reverts to the default value (VLAN 1).

Note Complete the steps in the "Completing Trunk Configuration" section on page 13-13 after performing the tasks in this section.

Configuring the 802.1Q Native VLAN

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 13-7 before performing the tasks in this section.

To configure the 802.1Q native VLAN, perform this task:

Command	Purpose
`Router(config-if)# switchport trunk native vlan vlan_ID`	(Optional) Configures the 802.1Q native VLAN. **Note** If VLAN locking is enabled, enter the VLAN name instead of the VLAN number. For more information, see the "VLAN Locking" section on page 17-9.
`Router(config-if)# no switchport trunk native vlan`	Reverts to the default value (VLAN 1).

When configuring the native VLAN, note the following information:

- The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 17-1 on page 17-2).
- The access VLAN is not automatically used as the native VLAN.

Note Complete the steps in the "Completing Trunk Configuration" section on page 13-13 after performing the tasks in this section.

Configuring the List of VLANs Allowed on a Trunk

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 13-7 before performing the tasks in this section.

To configure the list of VLANs allowed on a trunk, perform this task:

Command	Purpose
`Router(config-if)# switchport trunk allowed vlan {add | except | none | remove} vlan [,vlan[,vlan[,...]]`	(Optional) Configures the list of VLANs allowed on the trunk. **Note** If VLAN locking is enabled, enter VLAN names instead of VLAN numbers. For more information, see the "VLAN Locking" section on page 17-9.
`Router(config-if)# no switchport trunk allowed vlan`	Reverts to the default value (all VLANs allowed).

When configuring the list of VLANs allowed on a trunk, note the following information:

- The *vlan* parameter is either a single VLAN number from 1 through 4094, 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.
- If VLAN locking is enabled, enter VLAN names instead of VLAN numbers. When entering a range of VLAN names, you must leave spaces between the VLAN names and the dash.
- All VLANs are allowed by default.
- You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), Port Aggregation Protocol (PAgP), and DTP in VLAN 1.

Note Complete the steps in the "Completing Trunk Configuration" section on page 13-13 after performing the tasks in this section.

Configuring the List of Prune-Eligible VLANs

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 13-7 before performing the tasks in this section.

To configure the list of prune-eligible VLANs on the Layer 2 trunk, perform this task:

Command	Purpose
`Router(config-if)#` **`switchport trunk pruning vlan`** `{`**`none`** `|{{`**`add`** `|` **`except`** `|` **`remove`**`}` *`vlan`*`[,`*`vlan`*`[,`*`vlan`*`[,...]]}}`	(Optional) Configures the list of prune-eligible VLANs on the trunk (see the "Understanding VTP Pruning" section on page 16-3).
`Router(config-if)#` **`no switchport trunk pruning vlan`**	Reverts to the default value (all VLANs prune-eligible).

When configuring the list of prune-eligible VLANs on a trunk, note the following information:

- The *vlan* parameter is either a single VLAN number from 1 through 4094, except reserved VLANs (see Table 17-1 on page 17-2), 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.
- The default list of VLANs allowed to be pruned contains all VLANs.
- Network devices in VTP transparent mode do not send VTP Join messages. On trunk connections to network devices in VTP transparent mode, configure the VLANs used by the transparent-mode network devices or that need to be carried across the transparent-mode network devices as pruning ineligible.

Note Complete the steps in the "Completing Trunk Configuration" section on page 13-13 after performing the tasks in this section.

Completing Trunk Configuration

To complete Layer 2 trunk configuration, perform this task:

	Command	Purpose
Step 1	`Router(config-if)#` **`no shutdown`**	Activates the interface. (Required only if you shut down the interface.)
Step 2	`Router(config-if)#` **`end`**	Exits configuration mode.

Verifying Layer 2 Trunk Configuration

To verify Layer 2 trunk configuration, perform this task:

	Command	Purpose
Step 1	`Router# show running-config interface type[1] slot/port`	Displays the running configuration of the interface.
Step 2	`Router# show interfaces [type[1] slot/port] switchport`	Displays the switch port configuration of the interface.
Step 3	`Router# show interfaces [type[1] slot/port] trunk`	Displays the trunk configuration of the interface.

[1] *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Configuration and Verification Examples

This example shows how to configure the Fast Ethernet port 5/8 as an 802.1Q trunk. This example assumes that the neighbor port is configured to support 802.1Q trunking:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/8
Router(config-if)# shutdown
Router(config-if)# switchport
Router(config-if)# switchport mode dynamic desirable
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# no shutdown
Router(config-if)# end
Router# exit
```

This example shows how to verify the configuration:

```
Router# show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
 no ip address
 switchport
 switchport trunk encapsulation dot1q
end

Router# 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: ALL

Router# 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 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Router#
```

Configuring a LAN Interface as a Layer 2 Access Port

Note If you assign a LAN port to a VLAN that does not exist, the port is shut down until you create the VLAN in the VLAN database (see the "Creating or Modifying an Ethernet VLAN" section on page 17-10).

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

	Command	Purpose
Step 1	`Router(config)# **interface** *type*[1] *slot/port*`	Selects the LAN port to configure.
Step 2	`Router(config-if)# **shutdown**`	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3	`Router(config-if)# **switchport**`	Configures the LAN port for Layer 2 switching. **Note** You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional **switchport** commands with keywords.
Step 4	`Router(config-if)# **no switchport**`	Clears Layer 2 LAN port configuration.
Step 5	`Router(config-if)# **switchport mode access**`	Configures the LAN port as a Layer 2 access port.
	`Router(config-if)# **no switchport mode**`	Reverts to the default mode (**switchport mode dynamic desirable**).
Step 6	`Router(config-if)# **switchport access vlan** *vlan_ID*`	Places the LAN port in a VLAN. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 17-1 on page 17-2). **Note** If VLAN locking is enabled, enter the VLAN name instead of the VLAN number. For more information, see the "VLAN Locking" section on page 17-9.
	`Router(config-if)# **no switchport access vlan**`	Reverts to the default access VLAN (VLAN 1).
Step 7	`Router(config-if)# **no shutdown**`	Activates the interface. (Required only if you shut down the interface.)
Step 8	`Router(config-if)# **end**`	Exits configuration mode.

	Command	Purpose
Step 9	`Router#` **`show running-config interface`** `[`*`type`*[1] *`slot/port`*`]`	Displays the running configuration of the interface.
Step 10	`Router#` **`show interfaces`** `[`*`type`*[1] *`slot/port`*`]` **`switchport`**	Displays the switch port configuration of the interface.

[1] *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

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

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

This example shows how to verify the configuration:

```
Router# show running-config interface fastethernet 5/6
Building configuration...
!
Current configuration:
interface FastEthernet5/6
 no ip address
 switchport access vlan 200
 switchport mode access
end

Router# show interfaces fastethernet 5/6 switchport
Name: Fa5/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Enabled
Access Mode VLAN: 200 (VLAN0200)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL

Router#
```

Configuring a Custom IEEE 802.1Q EtherType Field Value

You can configure a custom EtherType field value on a port to support network devices that do not use the standard 0x8100 EtherType field value on 802.1Q-tagged or 802.1p-tagged frames.

To configure a custom value for the EtherType field, perform this task:

Command	Purpose
`Router(config-if)#` **`switchport dot1q ethertype`** *`value`*	Configures the 802.1Q EtherType field value for the port.
`Router(config-if)#` **`no switchport dot1q ethertype`**	Reverts to the default 802.1Q EtherType field value (0x8100).

When configuring a custom EtherType field value, note the following information:

- To use a custom EtherType field value, all network devices in the traffic path across the network must support the custom EtherType field value.
- You can configure a custom EtherType field value on trunk ports, access ports, and tunnel ports.
- You can configure a custom EtherType field value on the member ports of an EtherChannel.
- You cannot configure a custom EtherType field value on a port-channel interface.
- Each port supports only one EtherType field value. A port that is configured with a custom EtherType field value does not recognize frames that have any other EtherType field value as tagged frames. For example, a trunk port that is configured with a custom EtherType field value does not recognize the standard 0x8100 EtherType field value on 802.1Q-tagged frames and cannot put the frames into the VLAN to which they belong.

⚠ **Caution** A port that is configured with a custom EtherType field value considers frames that have any other EtherType field value to be untagged frames. A trunk port with a custom EtherType field value places frames with any other EtherType field value into the native VLAN. An access port or tunnel port with a custom EtherType field value places frames that are tagged with any other EtherType field value into the access VLAN. If you misconfigure a custom EtherType field value, frames might be placed into the wrong VLAN.

- See the *Release Notes for Cisco IOS Release 12.2(33)SXH and Later Releases* for a list of the modules that support custom IEEE 802.1Q EtherType field values.

This example shows how to configure the EtherType field value to 0x1234:

```
Router (config-if)# switchport dot1q ethertype 1234
Router (config-if)#
```