



## Configuring LAN Ports for Layer 2 Switching

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



### Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How Layer 2 Switching Works, page 7-1](#)
- [Default Layer 2 LAN Interface Configuration, page 7-5](#)
- [Layer 2 LAN Interface Configuration Guidelines and Restrictions, page 7-6](#)
- [Configuring LAN Interfaces for Layer 2 Switching, page 7-7](#)



### Note

To configure Layer 3 interfaces, see [Chapter 12, “Configuring Layer 3 Interfaces.”](#)

## Understanding How Layer 2 Switching Works

These sections describe how Layer 2 switching works on the Catalyst 6500 series switches:

- [Understanding Layer 2 Ethernet Switching, page 7-1](#)
- [Understanding VLAN Trunks, page 7-2](#)
- [Layer 2 LAN Port Modes, page 7-4](#)

## Understanding Layer 2 Ethernet Switching

These sections describe Layer 2 Ethernet switching:

- [Layer 2 Ethernet Switching Overview, page 7-2](#)
- [Switching Frames Between Segments, page 7-2](#)
- [Building the Address Table, page 7-2](#)

## Layer 2 Ethernet Switching Overview

Catalyst 6500 series 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.

Catalyst 6500 series switches solve 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 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 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 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 ports and to 200 Mbps for Fast Ethernet ports. Gigabit Ethernet ports on Catalyst 6500 series switches are full duplex only, providing 2-Gbps effective bandwidth.

## Switching Frames Between Segments

Each LAN port on a Catalyst 6500 series 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 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 station with the LAN port on which it was received.

## Building the Address Table

Catalyst 6500 series switches build the 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 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 16,000 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

These sections describe VLAN trunks on the Catalyst 6500 series switches:

- [Trunking Overview, page 7-3](#)
- [Encapsulation Types, page 7-4](#)

## Trunking Overview

**Note**

---

For information about VLANs, see [Chapter 9, “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-X6501-10GEX4
  - WS-X6502-10GE
  - WS-X6548-GE-TX
  - WS-X6548V-GE-TX
  - WS-X6148-GE-TX
  - WS-X6148V-GE-TX
- 

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

Ethernet trunk ports support several trunking modes (see [Table 7-2 on page 7-4](#)). 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 8, “Configuring VTP.”](#)

## Encapsulation Types

Table 7-1 lists the Ethernet trunk encapsulation types.

**Table 7-1 Ethernet Trunk Encapsulation Types**

Encapsulation	Function
<code>switchport trunk encapsulation isl</code>	Specifies ISL encapsulation on the trunk link. <b>Note</b> 10-Gigabit Ethernet ports do not support ISL encapsulation.
<code>switchport trunk encapsulation dot1q</code>	Specifies 802.1Q encapsulation on the trunk link.
<code>switchport trunk encapsulation negotiate</code>	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 7-2 lists the Layer 2 LAN port modes and describes how they function on LAN ports.

**Table 7-2 Layer 2 LAN Port Modes**

Mode	Function
<code>switchport mode access</code>	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.
<code>switchport mode dynamic desirable</code>	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 <b>trunk</b> , <b>desirable</b> , or <b>auto</b> mode. This is the default mode for all LAN ports.
<code>switchport mode dynamic auto</code>	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 <b>trunk</b> or <b>desirable</b> mode.
<code>switchport mode trunk</code>	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.
<code>switchport nonegotiate</code>	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 7-3 shows the Layer 2 LAN port default configuration.

**Table 7-3 Layer 2 LAN Interface Default Configuration**

Feature	Default
Interface mode: <ul style="list-style-type: none"> <li>• Before entering the <b>switchport</b> command</li> <li>• After entering the <b>switchport</b> command</li> </ul>	Layer 3 (unconfigured) <b>switchport mode dynamic desirable</b>
Trunk encapsulation	<b>switchport trunk encapsulation negotiate</b>
Allowed VLAN range	<ul style="list-style-type: none"> <li>• With Release 12.1(13)E and later releases, VLANs 1 to 4094, except reserved VLANs (see <a href="#">Table 9-1 on page 9-2</a>)</li> <li>• With 12.1 E releases earlier than Release 12.1(13)E, VLANs 1 to 1005</li> </ul>
VLAN range eligible for pruning	VLANs 2 to 1001
Default VLAN (for access ports)	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	<ul style="list-style-type: none"> <li>• 100 for 10-Mbps Ethernet LAN ports</li> <li>• 19 for 10/100-Mbps Fast Ethernet LAN ports</li> <li>• 19 for 100-Mbps Fast Ethernet LAN ports</li> <li>• 4 for 1,000-Mbps Gigabit Ethernet LAN ports</li> <li>• 2 for 10,000-Mbps 10-Gigabit Ethernet LAN ports</li> </ul>

# Layer 2 LAN Interface Configuration Guidelines and Restrictions

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

## Restrictions

- 10-Gigabit Ethernet ports do not support ISL encapsulation.
- 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.

## Guidelines

- 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).
- 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 will cause 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 on the Catalyst 6500 series switches:

- [Configuring a LAN Port for Layer 2 Switching, page 7-7](#)
- [Configuring a Layer 2 Switching Port as a Trunk, page 7-8](#)
- [Configuring a LAN Interface as a Layer 2 Access Port, page 7-14](#)



## Note

- Use the **default interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* command to revert an interface to its default configuration.
- With Release 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

## Configuring a LAN Port for Layer 2 Switching

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

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

1. *type* = ethernet, 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).

**Note**

When using the **switchport** command, if a port configured for Layer 3 is now configured for Layer 2, the configuration for Layer 3 is retained in the memory but not in the running configuration and is applied to the port whenever the port switches back to Layer 3. Also, if a port configured for Layer 2 is now configured for Layer 3, the configuration for Layer 2 is retained in the memory but not in the running configuration and is applied to the port whenever the port switches back to Layer 2. To restore the default configuration of the port in the memory and in the running configuration, use the **default interface** command. To avoid potential issues while changing the role of a port using the **switchport** command, shut down the interface before applying the **switchport** command.

## Configuring a Layer 2 Switching Port as a Trunk

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

- [Preparing a Layer 2 Switching Port for Configuration as a Trunk, page 7-8](#)
- [Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk, page 7-9](#)
- [Configuring the Layer 2 Trunk to Use DTP, page 7-9](#)
- [Configuring the Layer 2 Trunk Not to Use DTP, page 7-10](#)
- [Configuring the Default VLAN, page 7-10](#)
- [Configuring the 802.1Q Native VLAN, page 7-11](#)
- [Configuring the List of VLANs Allowed on a Trunk, page 7-11](#)
- [Configuring the List of Prune-Eligible VLANs, page 7-12](#)
- [Completing Trunk Configuration, page 7-13](#)
- [Verifying Layer 2 Trunk Configuration, page 7-13](#)
- [Configuration and Verification Examples, page 7-13](#)

## Preparing a Layer 2 Switching Port for Configuration as a Trunk

To prepare a Layer 2 switching port for configuration as a trunk, perform this task:

	Command	Purpose
<b>Step 1</b>	Router(config)# <b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i>	Selects the LAN port to configure.
<b>Step 2</b>	Router(config-if)# <b>shutdown</b>	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
<b>Step 3</b>	Router(config-if)# <b>switchport</b>	(Optional) Configures the LAN port for Layer 2 switching (required only if the LAN port is not already configured for Layer 2 switching; see the “ <a href="#">Configuring a LAN Port for Layer 2 Switching</a> ” section on page 7-7).

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

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



### Note

Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on [page 7-8](#) before performing the tasks in this section.

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

Command	Purpose
Router(config-if)# <b>switchport trunk encapsulation</b> {isl   dot1q   negotiate}	(Optional) Configures the encapsulation, which configures the Layer 2 switching port as either an ISL or 802.1Q trunk. <b>Note</b> To support the <b>switchport mode trunk</b> command, you must configure the encapsulation.
Router(config-if)# <b>no switchport trunk encapsulation</b>	Reverts to the default trunk encapsulation mode ( <b>negotiate</b> ).



### Note

Complete the steps in the “[Completing Trunk Configuration](#)” section on [page 7-13](#) after performing the tasks in this section.

## Configuring the Layer 2 Trunk to Use DTP



### Note

Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on [page 7-8](#) before performing the tasks in this section.

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

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

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

- Required only if the interface is a Layer 2 access port or to specify the trunking mode.
- See [Table 7-2 on page 7-4](#) for information about trunking modes.



### Note

Complete the steps in the “[Completing Trunk Configuration](#)” section on [page 7-13](#) after performing the tasks in this section.

## Configuring the Layer 2 Trunk Not to Use DTP


**Note**

Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on [page 7-8](#) before performing the tasks in this section.

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

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

When configuring the Layer 2 trunk not to use DTP, note the following syntax 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 7-9](#)).
- To support the **switchport nonegotiate** command, you must enter the **switchport mode trunk** command.
- Enter the **switchport mode dynamic trunk** command. See [Table 7-2 on page 7-4](#) 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 7-9](#)) 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 7-9](#)).


**Note**

Complete the steps in the “[Completing Trunk Configuration](#)” section on [page 7-13](#) after performing the tasks in this section.

## Configuring the Default VLAN


**Note**

Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on [page 7-8](#) before performing the tasks in this section.

To configure the default VLAN, perform this task:

Command	Purpose
Router(config-if)# <b>switchport access vlan</b> <i>vlan_ID</i>	(Optional) Configures the default VLAN, which is used if the interface stops trunking. <ul style="list-style-type: none"> <li>With Release 12.1(13)E and later releases, the <i>vlan_ID</i> value can be 1 to 4094, except for reserved VLANs (see <a href="#">Table 9-1 on page 9-2</a>).</li> <li>With 12.1 E releases earlier than Release 12.1(13)E, the <i>vlan_ID</i> value can be 1 to 1005.</li> </ul>
Router(config-if)# <b>no switchport access vlan</b>	Reverts to the default value (VLAN 1).

**Note**

Complete the steps in the [“Completing Trunk Configuration”](#) section on page 7-13 after performing the tasks in this section.

## Configuring the 802.1Q Native VLAN

**Note**

Complete the steps in the [“Preparing a Layer 2 Switching Port for Configuration as a Trunk”](#) section on page 7-8 before performing the tasks in this section.

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

Command	Purpose
Router(config-if)# <b>switchport trunk native vlan</b> <i>vlan_ID</i>	(Optional) Configures the 802.1Q native VLAN.
Router(config-if)# <b>no switchport trunk native vlan</b>	Reverts to the default value (VLAN 1).

When configuring the native VLAN, note the following syntax information:

- With Release 12.1(13)E and later releases, the *vlan\_ID* value can be 1 to 4094, except for reserved VLANs (see [Table 9-1 on page 9-2](#)).
- With 12.1 E releases earlier than Release 12.1(13)E, the *vlan\_ID* value can be 1 to 1005.
- The access VLAN is not automatically used as the native VLAN.

**Note**

Complete the steps in the [“Completing Trunk Configuration”](#) section on page 7-13 after performing the tasks in this section.

## Configuring the List of VLANs Allowed on a Trunk

**Note**

Complete the steps in the [“Preparing a Layer 2 Switching Port for Configuration as a Trunk”](#) section on page 7-8 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)# <b>switchport trunk allowed vlan</b> { <b>add</b>   <b>except</b>   <b>none</b>   <b>remove</b> } <i>vlan</i> [, <i>vlan</i> [, <i>vlan</i> [, ...]]]	(Optional) Configures the list of VLANs allowed on the trunk.
Router(config-if)# <b>no switchport trunk allowed vlan</b>	Reverts to the default value (all VLANs allowed).

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

- The *vlan* parameter is either a single VLAN ID or a range of VLAN IDs described by two VLAN IDs, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated *vlan* parameters or in dash-specified ranges.
- With Release 12.1(13)E and later releases, the VLAN IDs can be 1 to 4094, except for reserved VLANs (see [Table 9-1 on page 9-2](#)).
- With 12.1 E releases earlier than Release 12.1(13)E, the VLAN IDs can be 1 to 1005.
- All VLANs are allowed by default.
- With Release 12.1(13)E and later releases, you can remove the default VLANs (1002–1005) from a trunk. With earlier releases, you cannot remove any of the default VLANs from a trunk.
- With Release 12.1(11b)E or later, 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 7-13](#) after performing the tasks in this section.

## Configuring the List of Prune-Eligible VLANs

**Note**

Complete the steps in the [“Preparing a Layer 2 Switching Port for Configuration as a Trunk” section on page 7-8](#) 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)# <b>switchport trunk pruning vlan</b> { <b>none</b>   {{ <b>add</b>   <b>except</b>   <b>remove</b> }} <i>vlan</i> [, <i>vlan</i> [, <i>vlan</i> [, ...]]]	(Optional) Configures the list of prune-eligible VLANs on the trunk (see the <a href="#">“Understanding VTP Pruning” section on page 8-3</a> ).
Router(config-if)# <b>no switchport trunk pruning vlan</b>	Reverts to the default value (all VLANs prune-eligible).

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

- The *vlan* parameter is either a single VLAN ID or a range of VLAN IDs described by two VLAN IDs, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated *vlan* parameters or in dash-specified ranges.

- With Release 12.1(13)E and later releases, the VLAN IDs can be 1 to 4094, except for reserved VLANs (see [Table 9-1 on page 9-2](#)).
- With 12.1 E releases earlier than Release 12.1(13)E, the VLAN IDs can be 1 to 1005.
- 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 Catalyst 6500 series switches with 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 7-13](#) 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)# <b>no shutdown</b>	Activates the interface. (Required only if you shut down the interface.)
Step 2	Router(config-if)# <b>end</b>	Exits configuration mode.

## Verifying Layer 2 Trunk Configuration

To verify Layer 2 trunk configuration, perform this task:

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

1. *type* = ethernet, 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     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005

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

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 9-10).

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

	Command	Purpose
Step 1	Router(config)# <b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i>	Selects the LAN port to configure.
Step 2	Router(config-if)# <b>shutdown</b>	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.

	Command	Purpose
Step 3	Router(config-if)# <b>switchport</b>	Configures the LAN port for Layer 2 switching.  <b>Note</b> You must enter the <b>switchport</b> command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional <b>switchport</b> commands with keywords.
Step 4	Router(config-if)# <b>no switchport</b>	Clears Layer 2 LAN port configuration.
Step 5	Router(config-if)# <b>switchport mode access</b> Router(config-if)# <b>no switchport mode</b>	Configures the LAN port as a Layer 2 access port. Reverts to the default switchport mode ( <b>switchport mode dynamic desirable</b> ).
Step 6	Router(config-if)# <b>switchport access vlan vlan_ID</b>  Router(config-if)# <b>no switchport access vlan</b>	Places the LAN port in a VLAN. <ul style="list-style-type: none"><li>• With Release 12.1(13)E and later releases, the <i>vlan_ID</i> value can be 1 to 4094, except for reserved VLANs (see <a href="#">Table 9-1 on page 9-2</a>).</li><li>• With 12.1 E releases earlier than Release 12.1(13)E, the <i>vlan_ID</i> value can be 1 to 1005.</li></ul> Reverts to the default VLAN (VLAN 1).
Step 7	Router(config-if)# <b>no shutdown</b>	Activates the interface. (Required only if you shut down the interface.)
Step 8	Router(config-if)# <b>end</b>	Exits configuration mode.
Step 9	Router# <b>show running-config interface</b> [ <i>type</i> <sup>1</sup> <i>slot/port</i> ]	Displays the running configuration of the interface.
Step 10	Router# <b>show interfaces</b> [ <i>type</i> <sup>1</sup> <i>slot/port</i> ] <b>switchport</b>	Displays the switch port configuration of the interface.

1. *type* = ethernet, 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

With Release 12.1(20)E and later releases, 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)# <b>switchport dot1q ethertype</b> <i>value</i>	Configures the 802.1Q EtherType field value for the port.
Router(config-if)# <b>no switchport dot1q ethertype</b>	Reverts to the default 802.1Q EtherType field value (0x8100).

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

- 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.
- 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.

- You can configure a custom EtherType field value on these modules:
  - Supervisor engines
  - WS-X6516A-GBIC

- WS-X6516-GBIC



---

**Note** The WS-X6516A-GBIC and WS-X6516-GBIC modules apply a configured custom EtherType field value to all ports supported by each port ASIC (1 through 8 and 9 through 16).

---

- WS-X6516-GE-TX
  - WS-X6748-GE-TX
  - WS-X6724-SFP
  - WS-X6704-10GE
  - WS-X6816-GBIC
- You cannot configure a custom EtherType field value on the ports in an EtherChannel.
  - You cannot form an EtherChannel from ports that are configured with custom 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)#
```

