Cisco Press

Cisco Networking Academy Switched Networks Companion Guide: VLANs

Date: Jun 25, 2014 Sample Chapter is provided courtesy of Cisco Press.

This chapter covers how to configure, manage, and troubleshoot VLANs and VLAN trunks. It also examines security considerations and strategies relating to VLANs and trunks, and best practices for VLAN design.

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- How do you explain the purpose of VLANs in a switched network?
- How do you analyze the forwarding of frames by a switch based on VLAN configuration?
- How do you configure a switch port to be assigned to data and voice VLANs?
- How do you configure a trunk port on a LAN switch?
- How do you configure Dynamic Trunking Protocol (DTP)?
- How do you troubleshoot VLAN and trunk configurations in a switched network?
- How do you configure security features to mitigate attacks in a switched network?
- How do you explain security best practices for a switched network?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

- *Virtual Local-Area Network (VLAN) page 96*
- *VLAN Trunk page 96*
- *Data VLAN page 99*
- *User VLAN page 99*
- *Default VLAN page 100*
- *Native VLAN page 100*
- *IEEE 802.1Q page 100*
- *Management VLAN page 101*
- *Voice VLAN page 101*
- *Dynamic Trunking Protocol (DTP) page 120*
- *Switch Spoofing Attack page 138*
- *Double-Tagging Attack page 139*
- *Private VLAN (PVLAN) Edge page 140*
- *Protected Port page 140*
- *Black Hole VLAN page 142*

Introduction (3.0.1.1)

Network performance is an important factor in the productivity of an organization. One of the technologies used to improve network performance is the separation of large broadcast domains into smaller ones. By design, routers will block broadcast traffic at an interface. However, routers normally have a limited number of LAN interfaces. A router's primary role is to move information between networks, not provide network access to end devices.

The role of providing access into a LAN is normally reserved for an access layer switch. A *virtual local-area network (VLAN)* can be created on a Layer 2 switch to reduce the size of broadcast domains, similar to a Layer 3 device. VLANs are commonly incorporated into network design, making it easier for a network to support the goals of an organization. While VLANs are primarily used within switched local-area networks, modern implementations of VLANs allow them to span MANs and WANs.

This chapter will cover how to configure, manage, and troubleshoot VLANs and *VLAN trunks*. It will also examine security considerations and strategies relating to VLANs and trunks, and best practices for VLAN design.

Class Activity 3.0.1.2: Vacation Station

You have purchased a three-floor vacation home at the beach for rental purposes. The floor plan is identical on each floor. Each floor offers one digital television for renters to use.

According to the local Internet service provider, only three stations can be offered within a television package. It is your job to decide which television packages you offer your guests.

- Divide the class into groups of three students per group.
- Choose three different stations to make one subscription package for each floor of your rental home.
- Complete the PDF for this activity.
- Share your completed group-reflection answers with the class.

VLAN Segmentation (3.1)

LAN switches and VLANs go hand in hand. When you look at the configuration of a router, you do not see references to VLANs; however, when you look at the configuration of a switch, you see frequent references to VLANs. Modern switches are structured around VLANs. VLANs are to switches as networks are to routers. Almost everything you do on a switch relates to VLANs. So, to a large extent, learning about switching is learning about VLANs. The day in the future when every port on every switch is on a separate Layer 3 network is the day that VLANs are no longer necessary—the need for VLANs is tied to the need to put multiple switch ports in one broadcast domain (in one VLAN).

Overview of VLANs (3.1.1)

This section provides a high-level introduction to VLANs, which sets the stage for the chapter.

VLAN Definitions (3.1.1.1)

Within a switched internetwork, VLANs provide segmentation and organizational flexibility. VLANs provide a way to group devices within a LAN. A group of devices within a VLAN communicate as if they were attached to the same wire. VLANs are based on logical connections, instead of physical connections.

VLANs allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device, as seen in Figure 3-1. Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations within the VLAN where the packets are sourced. Each VLAN is considered a separate logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a device that supports routing.

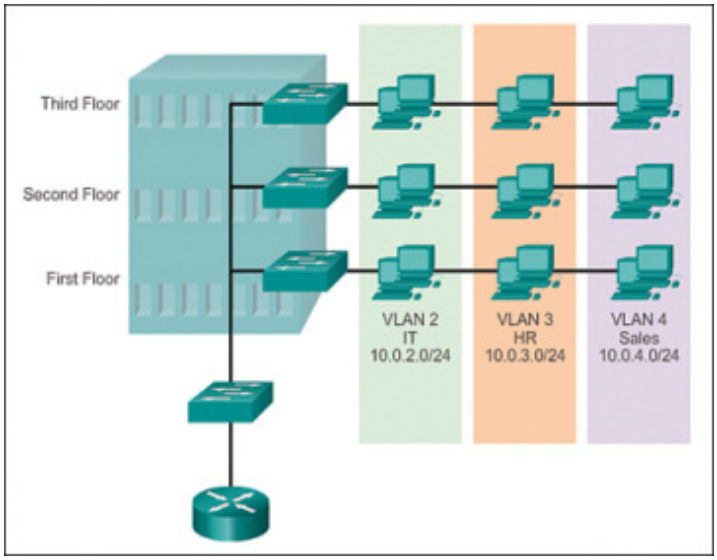

Figure 3-1 Defining VLAN Groups

A VLAN creates a logical broadcast domain that can span multiple physical LAN segments. VLANs improve network performance by separating large broadcast domains into smaller ones. If a device in one VLAN sends a broadcast Ethernet frame, all devices in the VLAN receive the frame, but devices in other VLANs do not.

VLANs enable the implementation of access and security policies according to specific groupings of users. Each switch port can be assigned to only one VLAN (with the exception of a port connected to an IP phone or to another switch).

Benefits of VLANs (3.1.1.2)

User productivity and network adaptability are important for business growth and success. VLANs make it easier to design a network to support the goals of an organization. The primary benefits of using VLANs are as follows:

- **Security:** Groups that have sensitive data are separated from the rest of the network, decreasing the chances of confidential information breaches. As shown in Figure 3-2, faculty computers are on VLAN 10 and completely separated from student and guest data traffic.

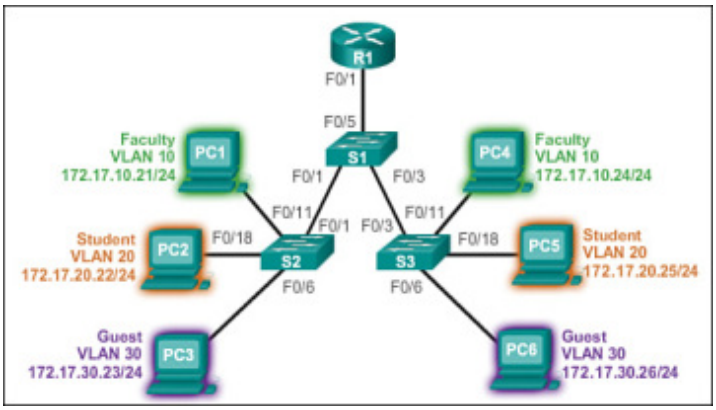

Figure 3-2 Benefits of VLANs

- **Cost reduction:** Cost savings result from reduced need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.
- **Better performance:** Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces unnecessary traffic on the network and boosts performance.
- **Shrink broadcast domains:** Dividing a network into VLANs reduces the number of devices in the broadcast domain. As shown in Figure 3-2, there are six computers on this network but there are three broadcast domains: Faculty, Student, and Guest.

- **Improved IT staff efficiency:** VLANs make it easier to manage the network because users with similar network requirements share the same VLAN. When a new switch is provisioned, all the policies and procedures already configured for the particular VLAN are implemented when the ports are assigned. It is also easy for the IT staff to identify the function of a VLAN by giving it an appropriate name. In Figure 3-2, for easy identification, VLAN 10 has been named "Faculty," VLAN 20 is named "Student," and VLAN 30 "Guest."
- **Simpler project and application management:** VLANs aggregate users and network devices to support business or geographic requirements. Having separate functions makes managing a project or working with a specialized application easier; an example of such an application is an e-learning development platform for faculty.

Each VLAN in a switched network corresponds to an IP network; therefore, VLAN design must take into consideration the implementation of a hierarchical network-addressing scheme. Hierarchical network addressing means that IP network numbers are applied to network segments or VLANs in an orderly fashion that takes the network as a whole into consideration. Blocks of contiguous network addresses are reserved for and configured on devices in a specific area of the network, as shown in Figure 3-2.

Types of VLANs (3.1.1.3)

There are a number of distinct types of VLANs used in modern networks. Some VLAN types are defined by traffic classes. Other types of VLANs are defined by the specific function that they serve.

Data VLAN

A ***data VLAN*** is a VLAN that is configured to carry user-generated traffic. A VLAN carrying voice or management traffic would not be a data VLAN. It is common practice to separate voice and management traffic from data traffic. A data VLAN is sometimes referred to as a ***user VLAN***. Data VLANs are used to separate the network into groups of users or devices.

Default VLAN

All switch ports become a part of the default VLAN after the initial bootup of a switch loading the default configuration. Switch ports that participate in the ***default VLAN*** are part of the same broadcast domain. This allows any device connected to any switch port to communicate with other devices on other switch ports. The default VLAN for Cisco switches is VLAN 1. In Example 3-1, the **show vlan brief** command was issued on a switch running the default configuration. Notice that all ports are assigned to VLAN 1 by default.

VLAN 1 has all the features of any VLAN, except it cannot be renamed or deleted. By default, all Layer 2 control traffic is associated with VLAN 1.

Example 3-1 Default VLAN Configuration

```
Switch# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
```

```
                                                Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Native VLAN

A *native VLAN* is assigned to an 802.1Q trunk port. Trunk ports are the links between switches that support the transmission of traffic associated with more than one VLAN. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic), as well as traffic that does not come from a VLAN (untagged traffic). Tagged traffic refers to traffic that has a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs. The 802.1Q trunk port places untagged traffic on the native VLAN, which by default is VLAN 1.

Native VLANs are defined in the *IEEE 802.1Q* specification to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. A native VLAN serves as a common identifier on opposite ends of a trunk link.

It is a best practice to configure the native VLAN as an unused VLAN, distinct from VLAN 1 and other VLANs. In fact, it is not unusual to dedicate a fixed VLAN to serve the role of the native VLAN for all trunk ports in the switched domain.

Management VLAN

A *management VLAN* is any VLAN configured to access the management capabilities of a switch. VLAN 1 is the management VLAN by default. To create the management VLAN, the switch virtual interface (SVI) of that VLAN is assigned an IP address and subnet mask, allowing the switch to be managed through HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 would be a bad choice for the management VLAN.

In the past, the management VLAN for a 2960 switch was the only active SVI. On 15.x versions of the Cisco IOS for Catalyst 2960 Series switches, it is possible to have more than one active SVI. With Cisco IOS Release 15.x, the particular active SVI assigned for remote management must be documented. While theoretically a switch can have more than one management VLAN, having more than one increases exposure to network attacks.

In Example 3-1, all ports are currently assigned to the default VLAN 1. No native VLAN is explicitly assigned and no other VLANs are active; therefore the network is designed with the native VLAN the same as the management VLAN. This is considered a security risk.

Voice VLANs (3.1.1.4)

A separate VLAN is needed to support Voice over IP (VoIP). VoIP traffic requires

- Assured bandwidth to ensure voice quality
- Transmission priority over other types of network traffic
- Ability to be routed around congested areas on the network
- Delay of less than 150 ms across the network

To meet these requirements, the entire network has to be designed to support VoIP. The details of how to configure a network to support VoIP are beyond the scope of this course, but it is useful to summarize how a *voice VLAN* works between a switch, a Cisco IP Phone, and a computer.

In Figure 3-3, VLAN 150 is designed to carry voice traffic. The student computer PC5 is attached to the Cisco IP Phone, and the phone is attached to switch S3.

PC5 is in VLAN 20, which is used for student data.

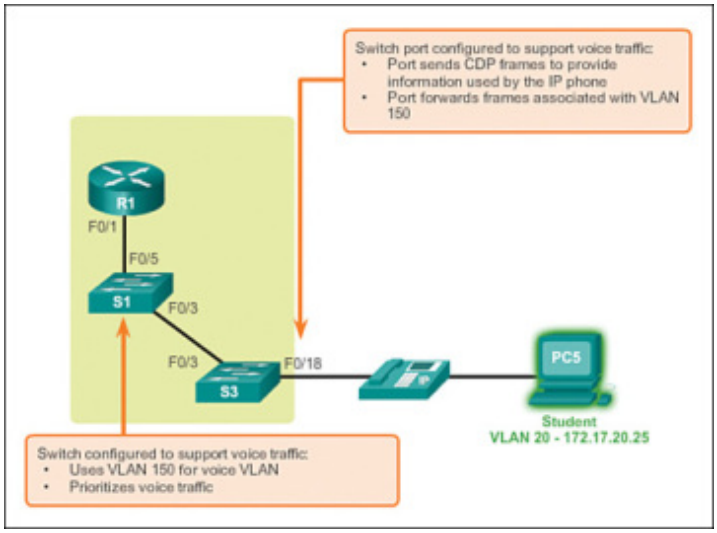

Figure 3-3 Voice VLAN

Packet Tracer Activity 3.1.1.5: Who Hears the Broadcast?

In this activity, a 24-port Catalyst 2960 switch is fully populated. All ports are in use. You will observe broadcast traffic in a VLAN implementation and answer some reflection questions.

VLANs in a Multiswitch Environment (3.1.2)

VLAN trunks are the connections in switched networks upon which all control traffic is transmitted and received. VLAN trunks carry data traffic for all VLANs in the switched network, unless restricted manually or with a pruning mechanism. Switches are interconnected with VLAN trunks. This section describes VLAN trunks.

VLAN Trunks (3.1.2.1)

A trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. Cisco supports IEEE 802.1Q for coordinating trunks on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces.

VLANs would not be very useful without VLAN trunks. VLAN trunks allow all VLAN traffic to propagate between switches so that devices that are in the same VLAN, but connected to different switches, can communicate without the intervention of a router.

A VLAN trunk does not belong to a specific VLAN; rather, it is a conduit for multiple VLANs between switches and routers. A trunk could also be used between a network device and server or other device that is equipped with an appropriate 802.1Q-capable NIC. By default, on a Cisco Catalyst switch, all VLANs are supported on a trunk port.

In Figure 3-4, the links between switches S1 and S2, and S1 and S3, are configured to transmit traffic coming from VLANs 10, 20, 30, and 99 across the network. This network could not function without VLAN trunks.

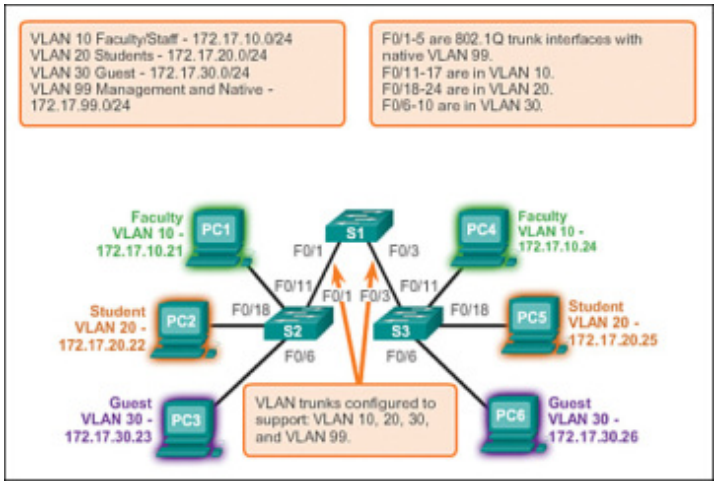

Figure 3-4 VLAN Trunks

Controlling Broadcast Domains with VLANs (3.1.2.2)

The behavior of broadcasts is affected by the presence of a switch. An ingress broadcast frame on a switch will only be forwarded out ports identified with the VLAN with which the frame is associated.

Network Without VLANs

In normal operation, when a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports except the port where the broadcast was received. In Figure 3-5, the entire network is configured in the same subnet (172.17.40.0/24) and no VLANs are configured. As a result, when the faculty computer (PC1) sends out a broadcast frame, switch S2 sends that broadcast frame out all of its ports. Eventually the entire network receives the broadcast because the network is one broadcast domain.

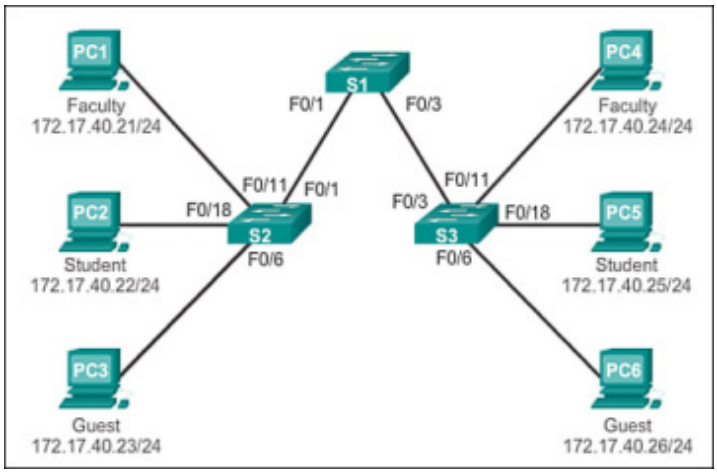

Figure 3-5 VLAN Trunks

Network with VLANs

As shown in Figure 3-6, the network has been segmented using two VLANs. Faculty devices are assigned to VLAN 10 and student devices are assigned to VLAN 20. When a broadcast frame is sent from the faculty computer, PC1, to switch S2, the switch forwards that broadcast frame only to those switch ports configured to support VLAN 10.

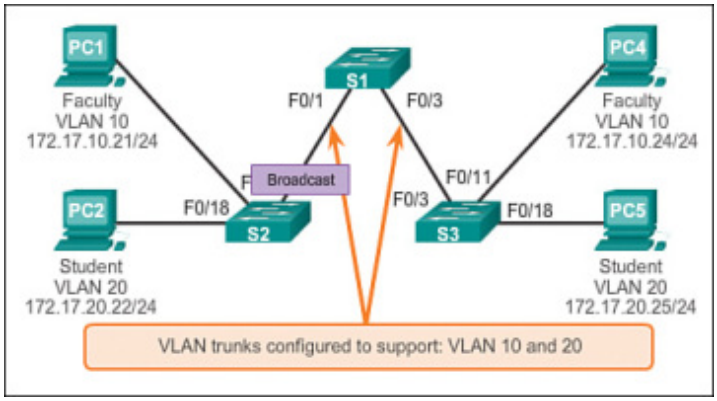

Figure 3-6 Broadcasts with VLAN Segmentation

The ports that comprise the connection between switches S2 and S1 (ports F0/1), and between S1 and S3 (ports F0/3), are trunks and have been configured to support all the VLANs in the network. Port F0/18 is associated with VLAN 20, so S2 forwards the broadcast out port F0/1 but does not forward the broadcast out port F0/18, as shown in Figure 3-6.

When S1 receives the broadcast frame on port F0/1, S1 forwards that broadcast frame out of the only other port configured to support VLAN 10, which is port F0/3. When S3 receives the broadcast frame on port F0/3, it forwards the broadcast frame out of the only other port configured to support VLAN 10, which is port F0/11. The broadcast frame arrives at the only other computer in the network configured in VLAN 10, which is faculty computer PC4.

When VLANs are implemented on a switch, the transmission of unicast, multicast, and broadcast traffic from a host in a particular VLAN is restricted to the devices that are in that VLAN.

Tagging Ethernet Frames for VLAN Identification (3.1.2.3)

Catalyst 2960 Series switches are Layer 2 devices. They use the Ethernet frame header information to forward packets. They do not have routing tables. The standard Ethernet frame header does not contain information about the VLAN to which the frame belongs. Thus, when Ethernet frames are placed on a trunk, information about the VLANs to which they belong must be added. This process, called tagging, is accomplished by using the IEEE 802.1Q header, specified in the IEEE 802.1Q standard. The 802.1Q header includes a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs.

When the switch receives a frame on a port configured in access mode and assigned a VLAN, the switch inserts a VLAN tag in the frame header, recalculates the FCS, and sends the tagged frame out of a trunk port.

VLAN Tag Field Details

The VLAN tag field, shown in Figure 3-7, consists of a Type field, a Priority field, a Canonical Format Identifier field, and VLAN ID field:

- **Type:** A 2-byte value called the tag protocol ID (TPID) value. For Ethernet, it is set to hexadecimal 0x8100.
- **Priority:** A 3-bit value that supports level or service implementation.
- **Canonical Format Identifier (CFI):** A 1-bit identifier that enables Token Ring frames to be carried across Ethernet links.

- **VLAN ID (VID):** A 12-bit VLAN identification number that supports up to 4096 VLAN IDs.

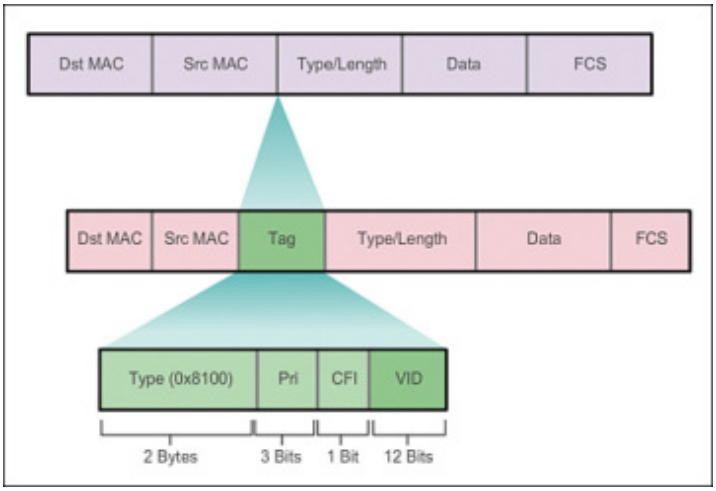

Figure 3-7 802.1Q VLAN Tag

After the switch inserts the Type and tag control information fields, it recalculates the FCS values and inserts the new FCS into the frame.

Native VLANs and 802.1Q Tagging (3.1.2.4)

The behavior of frames in the context of IEEE 802.1Q trunking is a vestige of the original standard, which was created when VLANs were still widely used. Essentially, the behavior is dictated by the assumption that a hub is connected between two switch ports that define a common VLAN trunk.

Tagged Frames on the Native VLAN

Some devices that support trunking add a VLAN tag to native VLAN traffic. Control traffic sent on the native VLAN should not be tagged. If an 802.1Q trunk port receives a tagged frame with the VLAN ID the same as the native VLAN, it drops the frame. Consequently, when configuring a switch port on a Cisco switch, configure devices so that they do not send tagged frames on the native VLAN. Devices from other vendors that support tagged frames on the native VLAN include IP phones, servers, routers, and non-Cisco switches.

Untagged Frames on the Native VLAN

When a Cisco switch trunk port receives untagged frames (which are unusual in a well-designed network), it forwards those frames to the native VLAN. If there are no devices associated with the native VLAN (which is not unusual) and there are no other trunk ports (which is not unusual), the frame is dropped. The default native VLAN is VLAN 1. When configuring an 802.1Q trunk port, a default Port VLAN ID (PVID) is assigned the value of the native VLAN ID. All untagged traffic coming into or out of the 802.1Q port is forwarded based on the PVID value. For example, if VLAN 99 is configured as the native VLAN, the PVID is 99 and all untagged traffic is forwarded to VLAN 99. If the native VLAN has not been reconfigured, the PVID value is set to VLAN 1.

In Figure 3-8, PC1 is connected by a hub to an 802.1Q trunk link. PC1 sends untagged traffic, which the switches associate with the native VLAN configured on the trunk ports, and forwards accordingly. Tagged traffic on the trunk received by PC1 is dropped. This scenario reflects poor network design for several reasons: It uses a hub, it has a host connected to a trunk link, and it implies that the switches have access ports assigned to the native VLAN. But it illustrates the motivation for the IEEE 802.1Q specification for native VLANs as a means of handling legacy scenarios.

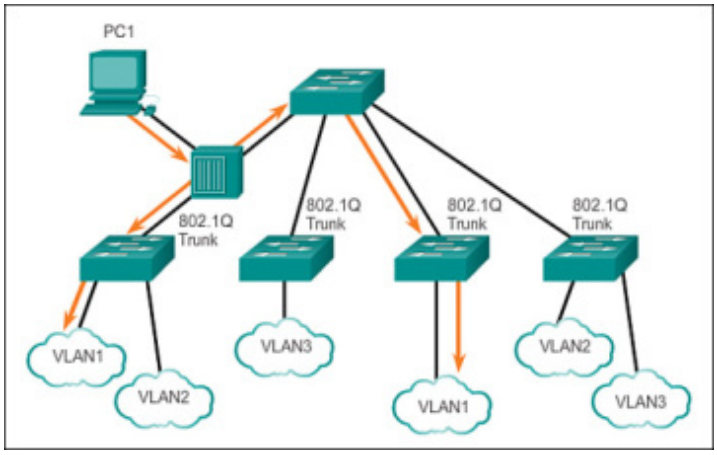

Figure 3-8 Native VLAN Forwarding Behavior

Voice VLAN Tagging (3.1.2.5)

Recall that to support VoIP, a separate voice VLAN is required.

An access port that is used to connect a Cisco IP Phone can be configured to use two separate VLANs: one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. The link between the switch and the IP phone acts as a trunk to carry both voice VLAN traffic and data VLAN traffic.

The Cisco IP Phone contains an integrated three-port 10/100 switch. The ports provide dedicated connections to these devices:

- Port 1 connects to the switch or other VoIP device.
- Port 2 is an internal 10/100 interface that carries the IP phone traffic.
- Port 3 (access port) connects to a PC or other device.

On the switch, the access is configured to send Cisco Discovery Protocol (CDP) packets that instruct an attached IP phone to send voice traffic to the switch in one of three ways, depending on the type of traffic:

- In a voice VLAN tagged with a Layer 2 class of service (CoS) priority value
- In an access VLAN tagged with a Layer 2 CoS priority value
- In an access VLAN, untagged (no Layer 2 CoS priority value)

In Figure 3-9, the student computer PC5 is attached to a Cisco IP Phone, and the phone is attached to switch S3. VLAN 150 is designed to carry voice traffic, while PC5 is in VLAN 20, which is used for student data.

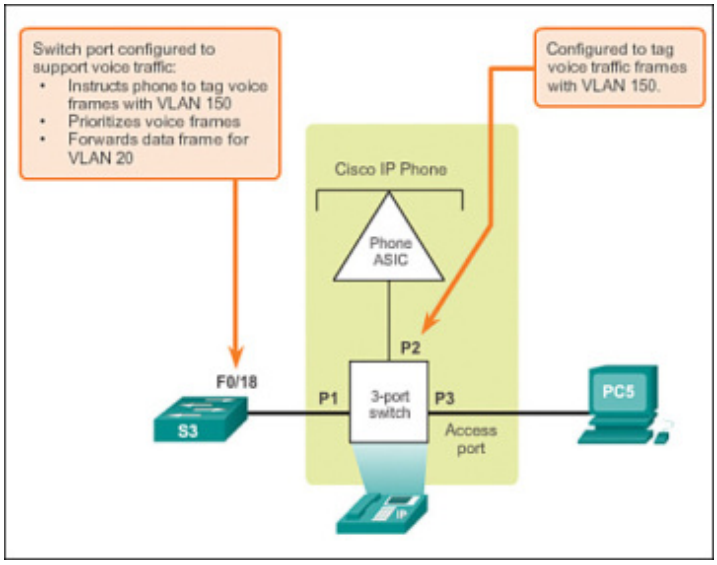

Figure 3-9 Voice VLAN Tagging

Sample Configuration

Example 3-2 shows sample output. A discussion of voice Cisco IOS commands is beyond the scope of this course, but the highlighted areas in the sample output show the F0/18 interface configured with a VLAN configured for data (VLAN 20) and a VLAN configured for voice (VLAN 150).

Example 3-2 Default VLAN Configuration

```
S1# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
<output omitted>
```

Activity 3.1.2.6: VLAN Trunks in Action

Go to the online course to perform this practice activity.

Packet Tracer Activity 3.1.2.7: Investigating a VLAN Implementation

In this activity, you will observe how broadcast traffic is forwarded by the switches when VLANs are configured and when VLANs are not configured.

VLAN Implementations (3.2)

Network administrators who are responsible for portions of the switched network are familiar with the basic configuration tasks related to creating VLANs, configuring trunk links, associating voice and data VLANs with ports, and securing the VLAN implementation. This section describes the major tasks required to configure VLANs and trunks on switches in the network infrastructure.

VLAN Assignment (3.2.1)

The first step in configuring VLANs is to create the VLANs and to associate switch ports with VLANs.

VLAN Ranges on Catalyst Switches (3.2.1.1)

Different Cisco Catalyst switches support various numbers of VLANs. The number of supported VLANs is large enough to accommodate the needs of most organizations. For example, the Catalyst 2960 and 3560 Series switches support over 4000 VLANs. Normal-range VLANs on these switches are numbered 1 to 1005, and extended-range VLANs are numbered 1006 to 4094. Catalyst 2960 switches running Cisco IOS Release 15.x support extended-range VLANs.

Normal-Range VLANs

Normal range VLANs are usually the ones utilized in switched networks, because most networks do not need over 1000 VLANs!

- Used in small- and medium-sized business and enterprise networks.
- Identified by a VLAN ID between 1 and 1005.
- IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- IDs 1 and 1002 to 1005 are automatically created and cannot be removed.
- Configurations are stored within a VLAN database file called vlan.dat. The vlan.dat file is located in the flash memory of the switch.
- The VLAN Trunking Protocol (VTP), which helps manage VLAN configurations between switches, can only learn and store normal-range VLANs.

Extended-Range VLANs

Extended range VLANs are primarily used in metropolitan service provider networks requiring over 1000 VLANs to support the various customers.

- Enable service providers to extend their infrastructure to a greater number of customers. Some global enterprises could be large enough to need extended-range VLAN IDs.
- Are identified by a VLAN ID between 1006 and 4094.
- Configurations are not written to the vlan.dat file.
- Support fewer VLAN features than normal-range VLANs.
- Are, by default, saved in the running configuration file.
- VTP does not learn extended-range VLANs.

NOTE

4096 is the upper bound for the number of VLANs available on Catalyst switches, because there are 12 bits in the VLAN ID field of the IEEE 802.1Q header.

Creating a VLAN (3.2.1.2)

When configuring normal-range VLANs, the configuration details are stored in flash memory on the switch in a file called vlan.dat. Flash memory is persistent and does not require the **copy running-config startup-config** command. However, because other details are often configured on a Cisco switch at the same time that VLANs are created, it is good practice to save running configuration changes to the startup configuration.

Table 3-1 displays the Cisco IOS command syntax used to add a VLAN to a switch and give it a name. Naming each VLAN is considered a best practice in switch configuration.

Table 3-1 Creating a VLAN

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Create a VLAN with a valid ID number.	S1(config)# **vlan vlan-id**
Specify a unique name to identify the VLAN.	S1(config-vlan)# **name vlan-name**
Return to privileged EXEC mode.	S1(config-vlan)# **end**

Figure 3-10 shows how the student VLAN (VLAN 20) is configured on switch S1. In the topology example, the student computer (PC2) has not been associated with a VLAN yet, but it does have an IP address of 172.17.20.22.

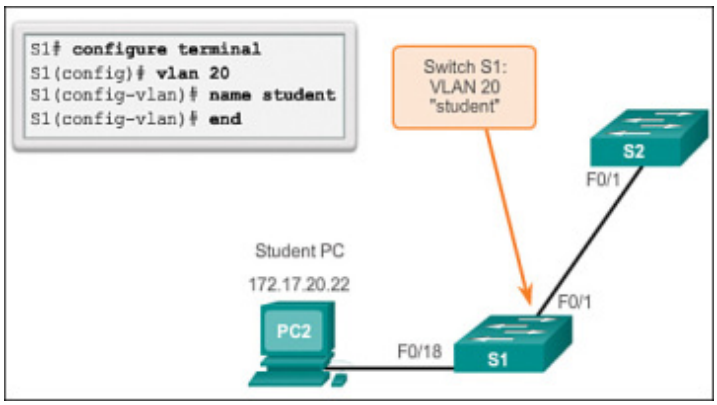

Figure 3-10 Sample VLAN Configuration

Activity 3.2.1.2: Creating and Verifying VLANs

Interactive Graphic

Go to the online course to use the Syntax Checker in the third graphic to create a VLAN and use the **show vlan brief** command to display the contents of the vlan.dat file.

In addition to entering a single VLAN ID, a series of VLAN IDs can be entered separated by commas, or a range of VLAN IDs separated by hyphens using the **vlan** *vlan-id* command. For example, use the following command to create VLANs 100, 102, 105, 106, and 107:

```
S1(config)# vlan 100,102,105-107
```

Assigning Ports to VLANs (3.2.1.3)

After creating a VLAN, the next step is to assign ports to the VLAN. An access port can belong to only one VLAN at a time. One exception to this rule is that of a port connected to an IP phone, in which case there are two VLANs associated with the port: one for voice and one for data.

Table 3-2 displays the syntax for defining a port to be an access port and assigning it to a VLAN. The **switchport mode access** command is optional but strongly recommended as a security best practice. With this command, the interface changes to permanent access mode.

Table 3-2 Assign Ports to VLANs

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface interface-id**
Set the port to access mode.	S1(config-if)# **switchport mode access**
Assign the port to a VLAN.	S1(config-if)# **switchport access vlan vlan-id**
Return to the privileged EXEC mode.	S1(config-if)# **end**

NOTE

Use the **interface range** command to simultaneously configure multiple interfaces.

In Figure 3-11, VLAN 20 is assigned to port F0/18 on switch S1; therefore, the student computer (PC2) is in VLAN 20. When VLAN 20 is configured on other switches, the network administrator knows to configure the other student computers to be in the same subnet as PC2 (172.17.20.0/24).

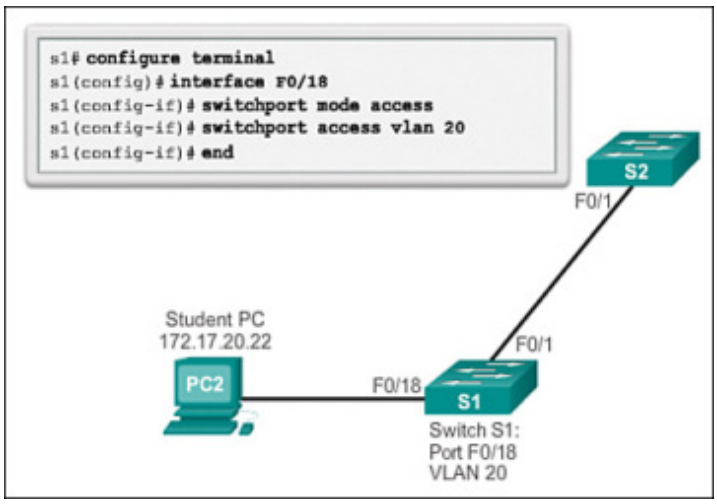

Figure 3-11 Sample Interface Configuration for VLANs

Activity 3.2.1.3: Assigning Ports to VLANs

Interactive Graphic

Go to the online course to use the Syntax Checker in the third graphic to assign a VLAN and use the **show vlan brief** command to display the contents of the vlan.dat file.

The **switchport access vlan** command forces the creation of a VLAN if it does not already exist on the switch. For example, VLAN 30 is not present in the **show vlan brief** output of the switch. If the **switchport access vlan 30** command is entered on any interface with no previous configuration, the switch displays

```
% Access VLAN does not exist. Creating vlan 30
```

Changing VLAN Port Membership (3.2.1.4)

There are a number of ways to change VLAN port membership. Table 3-3 shows the syntax for changing a switch port to VLAN 1 membership with the **no switchport access vlan** interface configuration mode command.

Table 3-3 Removing a VLAN Assignment

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface interface-id**
Remove the VLAN assignment from the port.	S1(config-if)# **no switchport access vlan**
Return to the privileged EXEC mode.	S1(config-if)# **end**

Interface F0/18 was previously assigned to VLAN 20. The **no switchport access vlan** command is entered for interface F0/18. Examine the output in the **show vlan brief** command, as shown in Example 3-3. The **show vlan brief** command displays the VLAN assignment and membership type for all switch ports. The **show vlan brief** command displays one line for each VLAN. The output for each VLAN includes the VLAN name, status, and switch ports.

Example 3-3 Sample VLAN Assignment Removal

```
S1(config)# interface f0/18
S1(config-if)# no switchport access vlan
S1(config-if)# do show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

VLAN 20 is still active, even though no ports are assigned to it. In Example 3-4, the show interfaces f0/18 switchport output verifies that the access VLAN for interface F0/18 has been reset to VLAN 1.

Example 3-4 Verification of VLAN Assignment Removal

```
S1# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
```

A port can easily have its VLAN membership changed. It is not necessary to first remove a port from a VLAN to change its VLAN membership. When an access port has its VLAN membership reassigned to another existing VLAN, the new VLAN membership simply replaces the previous VLAN membership. In Example 3-5, port F0/11 is assigned to VLAN 20.

Example 3-5 Changing VLAN Assignment

```
S1(config)# interface f0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
*Mar  31 09:33:26.058: %SYS-5-CONFIG_I: Configured from console by console
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
20   student                           active    Fa0/11
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1#
```

Activity 3.2.1.4: Creating and Verifying VLANs

Go to the online course to use the Syntax Checker in the fifth graphic to change VLAN port membership.

Deleting VLANs (3.2.1.5)

In Example 3-6, the **no vlan** *vlan-id* global configuration mode command is used to remove VLAN 20 from the switch. Switch S1 had a minimal configuration with all ports in VLAN 1 and an unused VLAN 20 in the VLAN database. The **show vlan brief** command verifies that VLAN 20 is no longer present in the vlan.dat file after using the **no vlan 20** command.

Example 3-6 Deleting a VLAN

```
S1(config)# no vlan 20
S1(config)# end
S1#
*Mar  1 07:37:55.785: %SYS-5-CONFIG_I: Configured from console by console
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

CAUTION

Before deleting a VLAN, be sure to first reassign all member ports to a different VLAN. Any ports that are not moved to an active VLAN are unable to communicate with other hosts after the VLAN is deleted and until they are assigned to an active VLAN.

Alternatively, the entire vlan.dat file can be deleted using the **delete flash:vlan.dat** privileged EXEC mode command. The abbreviated command version (**delete vlan.dat**) can be used if the vlan.dat file has not been moved from its default location. After issuing this command and reloading the switch, the previously configured VLANs are no longer present. This effectively places the switch into its factory default condition concerning VLAN configurations.

NOTE

For a Catalyst switch, the **erase startup-config** command must accompany the **delete vlan.dat** command prior to reload to restore the switch to its factory default condition.

Verifying VLAN Information (3.2.1.6)

After a VLAN is configured, VLAN configurations can be validated using Cisco IOS **show** commands.

Table 3-4 displays the show vlan command options.

Table 3-4 show vlan Command

Cisco IOS CLI Command Syntax show vlan [brief | id *vlan-id* | name *vlan-name* | summary]	
Display one line for each VLAN with the VLAN name, status, and its ports.	brief
Display information about a single VLAN identified by VLAN ID number. For *vlan-id*, the range is 1 to 4094.	id *vlan-id*
Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.	name *vlan-name*
Display VLAN summary information.	summary

Table 3-5 displays the show interfaces command options.

Table 3-5 show interfaces Command

Cisco IOS CLI Command Syntax show interfaces [*interface-id* | vlan *vlan-id*] | switchport	
Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 6.	*interface-id*
VLAN identification. The range is 1 to 4095.	vlan *vlan-id*
Display the administrative and operational status of a switching port, including port blocking and port protection settings.	switchport

In Example 3-7, the show vlan name student command produces output that is not easily interpreted. The preferable option is to use the show vlan brief command. The show vlan summary command displays the count of all configured VLANs. The output in Example 3-7 shows seven VLANs.

Example 3-7 Using the show vlan Command

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------
20   student                           active    Fa0/11
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------

S1# show vlan summary
Number of existing VLANs           : 7
 Number of existing VTP VLANs      : 7
 Number of existing extended VLANs : 0
```

The show interfaces vlan *vlan-id* command displays details that are beyond the scope of this course. The important information appears on the second line in Example 3-8, indicating that VLAN 20 is up.

Example 3-8 Using the show interfaces vlan Command

```
S1# show interfaces vlan 20
Vlan 20 is up, line protocol is down
  Hardware is EtherSVI, address is 0021.a1e0.78c1 (bia 0021.a1e0.78c1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
S1#
```

Activity 3.2.1.6: Using the show interfaces Command

Go to the online course to use the Syntax Checker in the fourth graphic to display the VLAN and switch port information, and verify VLAN assignments and mode.

Packet Tracer Activity 3.2.1.7: Configuring VLANs

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

VLAN Trunks (3.2.2)

In this section, the elements of VLAN trunk configuration are explored. Remember that VLAN trunks carry all the control traffic between switches. VLAN trunks enable the communication between switches required for many of the technologies specific to the LAN switched environment.

Configuring IEEE 802.1Q Trunk Links (3.2.2.1)

A VLAN trunk is an OSI Layer 2 link between two switches that carries traffic for all VLANs (unless the allowed VLAN list is restricted manually or dynamically). To enable trunk links, configure the ports on either end of the physical link with parallel sets of commands.

To configure a switch port on one end of a trunk link, use the **switchport mode trunk** command. With this command, the interface changes to permanent trunking mode. The port enters into a ***Dynamic Trunking Protocol (DTP)*** negotiation to convert the link into a trunk link even if the interface connecting to it does not agree to the change. DTP is described in the next topic. In this course, the

switchport mode trunk command is the only method implemented for trunk configuration.

The Cisco IOS command syntax to specify a native VLAN (other than VLAN 1) is shown in Table 3-6.

Table 3-6 802.1Q Trunk Configuration

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface** *interface-id*
Force the link to be a trunk link.	S1(config-if)# **switchport mode trunk**
Specify a native VLAN for 802.1Q trunks.	S1(config-if)# **switchport trunk native vlan** vlan-id
Specify the list of VLANs to be allowed on the trunk link.	S1(config-if)# **switchport trunk allowed vlan** *vlan-list*
Return to the privileged EXEC mode.	S1(config-if)# **end**

Use the Cisco IOS **switchport trunk allowed vlan** *vlan-list* command to specify the list of VLANs to be allowed on the trunk link.

In Figure 3-12, VLANs 10, 20, and 30 support the Faculty, Student, and Guest computers (PC1, PC2, and PC3). The native VLAN should also be changed from VLAN 1 and changed to another VLAN such as VLAN 99. By default, all VLANs are allowed across a trunk link. The **switchport trunk allowed vlan** command can be used to limit the allowed VLANs.

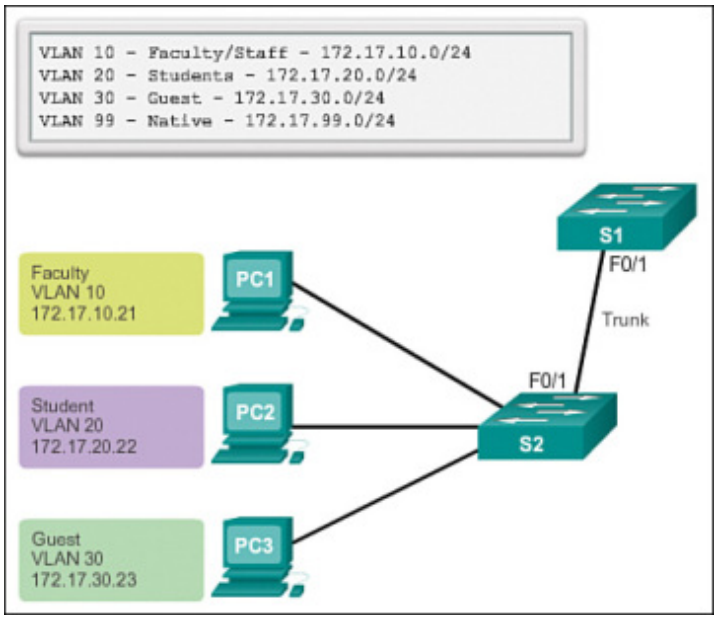

Figure 3-12 Sample Interface Configuration for VLANs

In Example 3-9, the F0/1 port on switch S1 is configured as a trunk port, assigns the native VLAN to VLAN 99, and specifies the trunk to only forward traffic for VLANs 10, 20, 30, and 99.

Example 3-9 Sample Trunk Configuration

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

NOTE

This configuration assumes the use of Cisco Catalyst 2960 switches, which automatically use 802.1Q encapsulation on trunk links. Other switches might require manual configuration of the encapsulation. Always configure both ends of a trunk link with the same native VLAN. If 802.1Q trunk configuration is not the same on both ends, Cisco IOS Software reports errors.

Resetting the Trunk to the Default State (3.2.2.2)

Table 3-7 shows the commands to remove the allowed VLANs and reset the native VLAN of the trunk. When reset to the default state, the trunk allows all VLANs and uses VLAN 1 as the native VLAN.

Table 3-7 Resetting Configured Values on Trunk Links

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode.	S1(config)# interface interface-id
Force the link to be a trunk link.	S1(config-if)# no switchport trunk allowed vlan
Specify a native VLAN for 802.1Q trunks.	S1(config-if)# no switchport trunk native vlan
Return to the privileged EXEC mode.	S1(config-if)# end

Example 3-10 shows the commands used to reset all trunking characteristics of a trunking interface to the default settings. The show interfaces f0/1 switchport command reveals that the trunk has been reconfigured to a default state.

Example 3-10 Resetting Trunk Link

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

In Example 3-11, the sample output shows the commands used to remove the trunk feature from the F0/1 switch port on switch S1. The show interfaces f0/1 switchport command reveals that the F0/1 interface is now in static access mode.

Example 3-11 Return Port to Access Mode

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
```

```
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

Verifying Trunk Configuration (3.2.2.3)

Example 3-12 displays the configuration of switch port F0/1 on switch S1. The configuration is verified with the **show interfaces** *interface-id* **switchport** command.

Example 3-12 Verifying Trunk Configuration

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

The top highlighted area shows that port F0/1 has its administrative mode set to **trunk**. The port is in trunking mode. The next highlighted area verifies that the native VLAN is VLAN 99. Farther down in the output, the bottom highlighted area shows that all VLANs are enabled on the trunk.

Activity 3.2.2.3: Configuring and Verifying a VLAN Trunk

Go to the online course to use the Syntax Checker in the second graphic to configure a trunk supporting all VLANs on interface F0/1 with native VLAN 99. Verify the trunk configuration with the **show interfaces f0/1 switchport** command.

Packet Tracer Activity 3.2.2.4: Configuring Trunks

Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs. This activity focuses on creating trunk ports and assigning them to a native VLAN other than the default.

Lab 3.2.2.5: Configuring VLANs and Trunking

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Create VLANs and Assign Switch Ports
- Part 3: Maintain VLAN Port Assignments and the VLAN Database
- Part 4: Configure an 802.1Q Trunk Between the Switches
- Part 5: Delete the VLAN Database

Dynamic Trunking Protocol (3.2.3)

Networking technologies often involve both manual and automatic implementations. For example, routing, speed/duplex port configuration, and cable selection versus auto-MDIX illustrate this dichotomy of manual versus automatic. In LAN switching, Dynamic Trunking Protocol (DTP) is one of the first examples one encounters of manual versus automatic. With DTP, network administrators have the option to let neighboring switches autonegotiate trunk formation.

Introduction to DTP (3.2.3.1)

Ethernet trunk interfaces support different trunking modes. An interface can be set to trunking or nontrunking, or to negotiate trunking with the neighbor interface. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis only between network devices.

DTP is a Cisco-proprietary protocol that is automatically enabled on Catalyst 2960 and Catalyst 3560 Series switches. Switches from other vendors do not support DTP. DTP manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP.

CAUTION

Some internetworking devices might forward DTP frames improperly, which can cause misconfigurations. To avoid this, turn off DTP on interfaces on a Cisco switch connected to devices that do not support DTP.

The default DTP configuration for Cisco Catalyst 2960 and 3560 switches is dynamic auto, as shown in Figure 3-13 on interface F0/3 of switches S1 and S3.

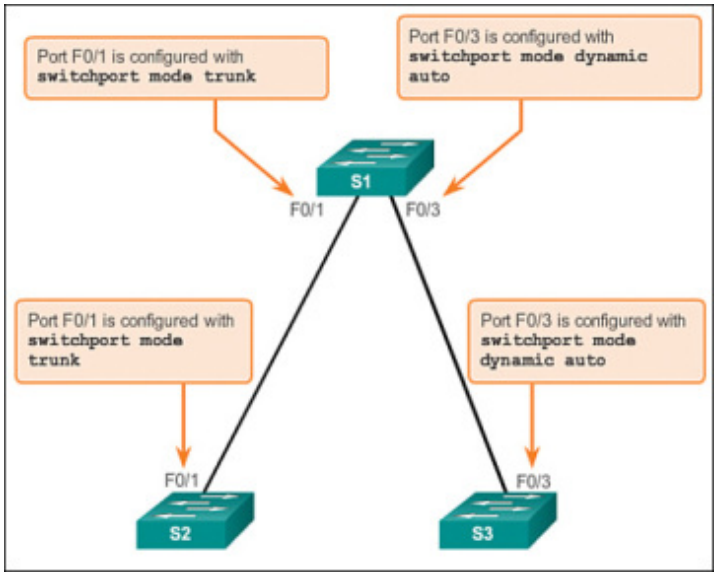

Figure 3-13 Initial DTP Configuration

To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. This causes the interface to become a trunk, but not generate DTP frames.

In Figure 3-14, the link between switches S1 and S2 becomes a trunk because the F0/1 ports on switches S1 and S2 are configured to ignore all DTP advertisements, and to come up in and stay in trunk port mode. The F0/3 ports on switches S1 and S3 are set to dynamic auto, so the negotiation results in the access mode state. This creates an inactive trunk link. When configuring a port to be in trunk mode, use the **switchport mode trunk** command. There is no ambiguity about which state the trunk is in; it is always on. With this configuration, it is easy to remember which state the trunk ports are in; if the port is supposed to be a trunk, the mode is set to trunk.

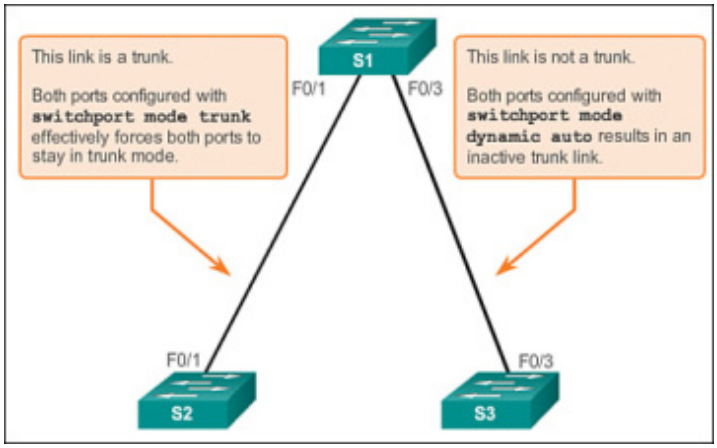

Figure 3-14 DTP Interaction Results

Negotiated Interface Modes (3.2.3.2)

Ethernet interfaces on Catalyst 2960 and Catalyst 3560 Series switches support different trunking modes with the help of DTP:

- **switchport mode access:** Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface, regardless of whether the neighboring interface is a trunk interface.
- **switchport mode dynamic auto:** Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. The default switch port mode for all Ethernet interfaces is **dynamic auto**.

- **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. This is the default switch port mode on older switches, such as the Catalyst 2950 and 3550 Series switches.
- **switchport mode trunk:** Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.
- **switchport nonegotiate:** Prevents the interface from generating DTP frames. You can use this command only when the interface switch port mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

Table 3-8 illustrates the results of the DTP configuration options on opposite ends of a trunk link connected to Catalyst 2960 switch ports.

Table 3-8 DTP-Negotiated Interface Modes

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Trunk

Configure trunk links statically whenever possible. The default DTP mode is dependent on the Cisco IOS Software version and on the platform. To determine the current DTP mode, issue the **show dtp interface** command, as shown in Example 3-13.

Example 3-13 Verifying DTP Mode

```
S1# show dtp interface f0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:                              TRUNK/ON/TRUNK
  TOT/TAT/TNT:                              802.1Q/802.1Q/802.1Q
  Neighbor address 1:                       0CD996D23F81
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       12/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S6:TRUNK
  # times multi & trunk                     0
  Enabled:                                  yes
  In STP:
<output omitted>
```

Activity 3.2.3.2: Verifying DTP Mode

Go to the online course to use the Syntax Checker in the third graphic to determine the DTP mode on interface F0/1.

NOTE

A general best practice is to set the interface to **trunk** and **nonegotiate** when a trunk link is required. On links where trunking is not intended, DTP should be turned off.

Activity 3.2.3.3: Predict DTP Behavior

Interactive Graphic

Go to the online course to perform this practice activity.

Troubleshoot VLANs and Trunks (3.2.4)

A network administrator responsible for portions of the switched infrastructure is able to quickly diagnose and solve problems. Troubleshooting VLANs and VLAN trunks is standard practice in a switched environment.

IP Addressing Issues with VLAN (3.2.4.1)

Each VLAN must correspond to a unique IP subnet. If two devices in the same VLAN have different subnet addresses, they cannot communicate. This is a common problem, and it is easy to solve by identifying the incorrect configuration and changing the subnet address to the correct one.

In Figure 3-15, PC1 cannot connect to the Web/TFTP server shown.

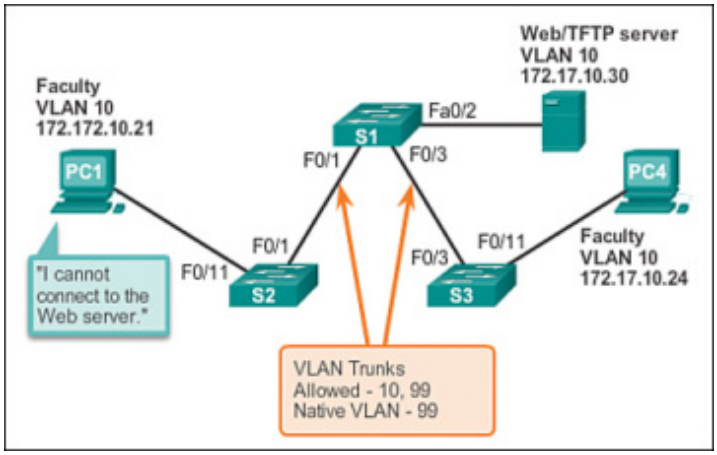

Figure 3-15 IP Issue Within VLAN

A check of the IP configuration settings of PC1 shown in Example 3-14 reveals the most common error in configuring VLANs: an incorrectly configured IP address. PC1 is configured with an IP address of 172.172.10.21, but it should have been configured with 172.17.10.21.

Example 3-14 Problem: Incorrect IP Address

```
PC1> ipconfig
   IPv4 Address. . . . . . . . . . . : 172.172.10.21
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 0.0.0.0
```

The PC1 Fast Ethernet configuration dialog box shows the updated IP address of 172.17.10.21. In Figure 3-16, the output on the bottom reveals that PC1 has regained connectivity to the Web/TFTP server found at IP address 172.17.10.30.

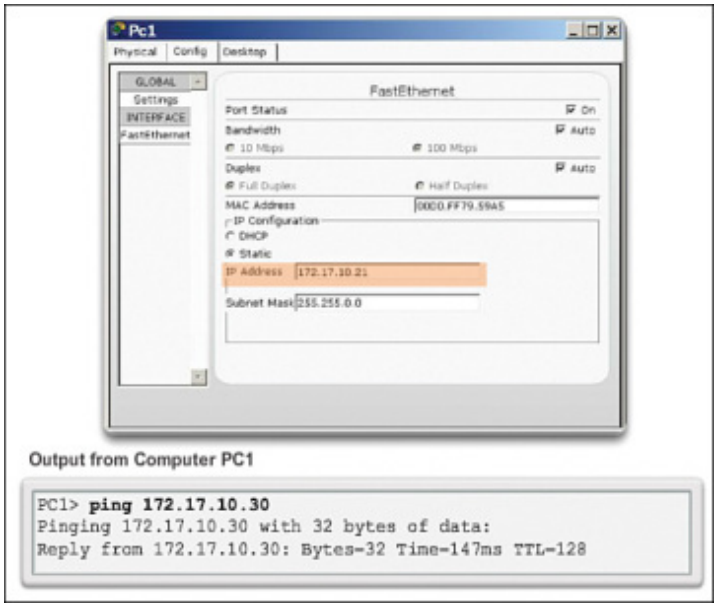

Figure 3-16 Solution: Change PC IP Address

Missing VLANs (3.2.4.2)

If there is still no connection between devices in a VLAN, but IP addressing issues have been ruled out, refer to the flowchart in Figure 3-17 to troubleshoot:

- **Step 1.** Use the **show vlan** command to check whether the port belongs to the expected VLAN. If the port is assigned to the wrong VLAN, use the **switchport access vlan** command to correct the VLAN membership. Use the **show mac address-table** command to check which addresses were learned on a particular port of the switch and to which VLAN that port is assigned.
- **Step 2.** If the VLAN to which the port is assigned is deleted, the port becomes inactive. Use the **show vlan** or **show interfaces switchport** command.

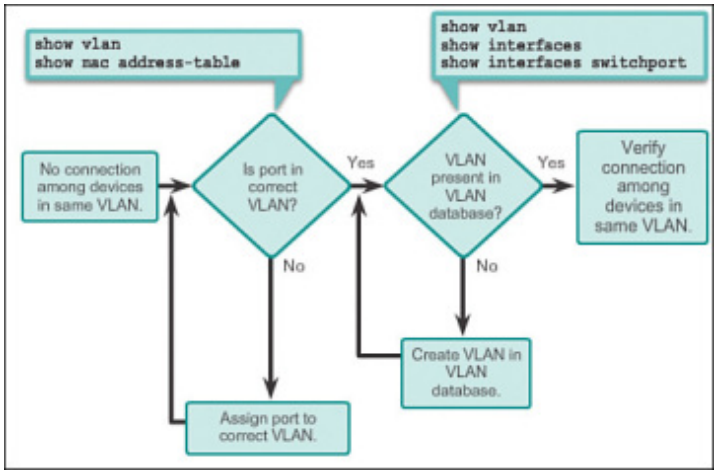

Figure 3-17 Missing VLAN

To display the MAC address table, use the **show macaddress-table** command. Example 3-15 shows MAC addresses that were learned on the F0/1 interface. It can be seen that MAC address 000c.296a.a21c was learned on interface F0/1 in VLAN 10. If this number is not the expected VLAN number, change the port VLAN membership using the **switchport access vlan** command.

Example 3-15 Missing VLAN

```
S1# show mac address-table interface FastEthernet 0/1
          Mac Address Table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    000c.296a.a21c    DYNAMIC     Fa0/1
  10    000f.34f9.9181    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 2
S1# show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Each port in a switch belongs to a VLAN. If the VLAN to which the port belongs is deleted, the port becomes inactive. All ports belonging to the VLAN that was deleted are unable to communicate with the rest of the network. Use the **show interface f0/1 switchport** command to check whether the port is inactive. If the port is inactive, it is not functional until the missing VLAN is created using the **vlan** *vlan-id* command.

Introduction to Troubleshooting Trunks (3.2.4.3)

A common task of a network administrator is to troubleshoot trunk link formation or links incorrectly behaving as trunk links. Sometimes a switch port can behave like a trunk port even if it is not configured as a trunk port. For example, an access port might accept frames from VLANs different from the VLAN to which it is assigned. This is called VLAN leaking.

Figure 3-18 displays a flowchart of general trunk troubleshooting guidelines.

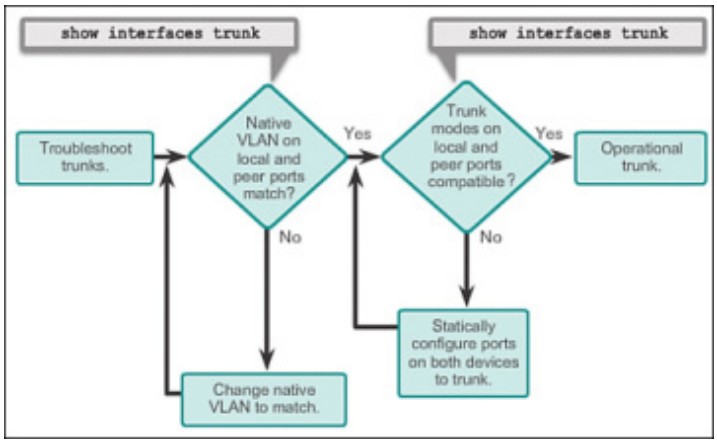

Figure 3-18 Troubleshooting Trunks

To troubleshoot issues when a trunk is not forming or when VLAN leaking is occurring, proceed as follows:

- **Step 1.** Use the **show interfaces trunk** command to check whether the local and peer native VLANs match. If the native VLAN does not match on

both sides, VLAN leaking occurs.

- **Step 2.** Use the **show interfaces trunk** command to check whether a trunk has been established between switches. Statically configure trunk links whenever possible. Cisco Catalyst switch ports use DTP by default and attempt to negotiate a trunk link.

To display the status of the trunk and to display the native VLAN used on that trunk link, and to verify trunk establishment, use the **show interfaces trunk** command. Example 3-16 shows that the native VLAN on one side of the trunk link was changed to VLAN 2. If one end of the trunk is configured as native VLAN 99 and the other end is configured as native VLAN 2, a frame sent from VLAN 99 on one side is received on VLAN 2 on the other side. VLAN 99 leaks into the VLAN 2 segment.

Example 3-16 Troubleshooting Trunks

```
S1# show interfaces f0/1 trunk

Port        Mode             Encapsulation  Status              Native vlan
Fa0/1       auto             802.1q         trunking            2
<output omitted>
```

CDP displays a notification of a native VLAN mismatch on a trunk link with this message:

```
*Mar 1 06:45:26.232: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).
```

Connectivity issues occur in the network if a native VLAN mismatch exists. Data traffic for VLANs, other than the two native VLANs configured, successfully propagates across the trunk link, but data associated with either of the native VLANs does not successfully propagate across the trunk link.

As shown in Example 3-16, native VLAN mismatch issues do not keep the trunk from forming. To solve the native VLAN mismatch, configure the native VLAN to be the same VLAN on both sides of the link.

Common Problems with Trunks (3.2.4.4)

Trunking issues are usually associated with incorrect configurations. When configuring VLANs and trunks on a switched infrastructure, the following types of configuration errors are the most common:

- **Native VLAN mismatches:** Trunk ports are configured with different native VLANs. This configuration error generates console notifications, and causes control and management traffic to be misdirected. This poses a security risk. For example, one port might be configured with VLAN 99 and the other with VLAN 100.
- **Trunk mode mismatches:** One trunk port is configured in a mode that is not compatible for trunking on the corresponding peer port. This configuration error causes the trunk link to stop working. For example, both local and peer switch port modes might be configured as dynamic auto.
- **Allowed VLANs on trunks:** The list of allowed VLANs on a trunk has not been updated with the current VLAN trunking requirements. In this situation, unexpected traffic or no traffic is being sent over the trunk. For example, the list of allowed VLANs might not support current VLAN trunking requirements.

If an issue with a trunk is discovered and if the cause is unknown, start troubleshooting by examining the trunks for a native VLAN mismatch. If that is not the cause, check for trunk mode mismatches, and finally check for the allowed VLAN list on the trunk. The next several sections examine how to fix the common problems with trunks.

Trunk Mode Mismatches (3.2.4.5)

Trunk links are normally configured statically with the **switchport mode trunk** command. Cisco Catalyst switch trunk ports use DTP to negotiate the state of the link. When a port on a trunk link is configured with a trunk mode that is incompatible with the neighboring trunk port, a trunk link fails to form between the two switches.

In the scenario illustrated in Figure 3-19, PC4 cannot connect to the internal web server. The topology indicates a valid configuration. Why is there a problem?

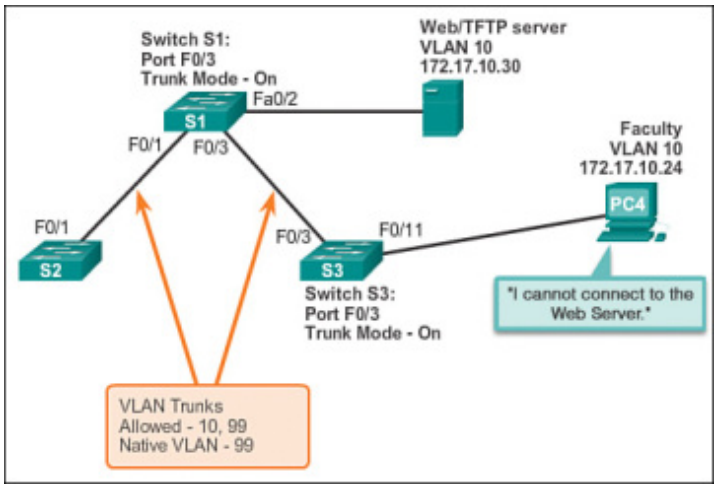

Figure 3-19 Scenario Topology

Check the status of the trunk ports on switch S1 using the **show interfaces trunk** command. The output shown in Example 3-17 reveals that interface Fa0/3 on switch S1 is not currently a trunk link. Examining the F0/3 interface reveals that the switch port is actually in dynamic auto mode. An examination of the trunks on switch S3 reveals that there are no active trunk ports. Further checking reveals that the Fa0/3 interface is also in dynamic auto mode. This explains why the trunk is down.

Example 3-17 Mismatched DTP Modes

```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
<output omitted>
S3# show interfaces trunk
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
<output omitted>
```

To resolve the issue, reconfigure the trunk mode of the F0/3 ports on switches S1 and S3, as shown in Example 3-18. After the configuration change, the output of the **show interfaces** command indicates that the port on switch S1 is now in trunking mode. The output from PC4 indicates that it has regained connectivity to the Web/TFTP server found at IP address 172.17.10.30.

Example 3-18 Corrected Trunk Modes

```
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<output omitted>
S3(config)# interface f0/3
S3(config-if)# switchport mode trunk
S3(config-if)# end
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<output omitted>
S3# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/3       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/3       10,99

Port        Vlans allowed and active in management domain
Fa0/3       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,99
PC4> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
<output omitted>
```

Incorrect VLAN List (3.2.4.6)

For traffic from a VLAN to be transmitted across a trunk, it must be allowed on the trunk. To do so, use the **switchport trunk allowed vlan** *vlan-id* command.

In Figure 3-20, VLAN 20 (Student) and PC5 have been added to the network. The documentation has been updated to show that the VLANs allowed on the trunk are 10, 20, and 99. In this scenario, PC5 cannot connect to the student email server.

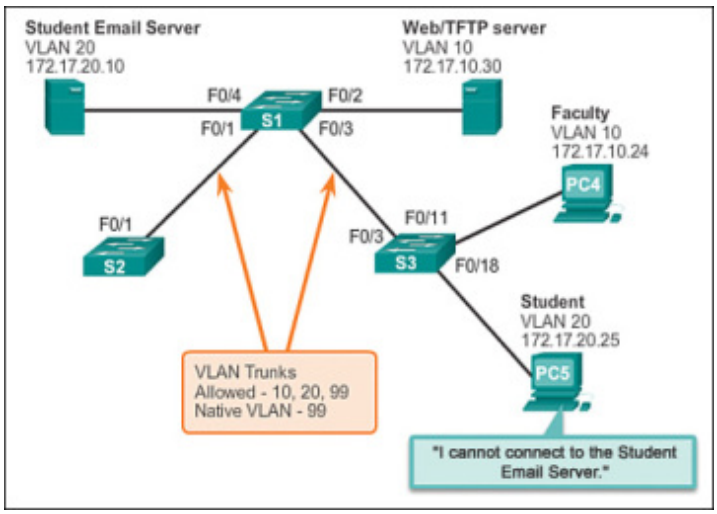

Figure 3-20 Scenario Topology

Check the trunk ports on switch S1 using the show interfaces trunk command, as shown in Example 3-19. The command reveals that the interface F0/3 on switch S3 is correctly configured to allow VLANs 10, 20, and 99. An examination of the F0/3 interface on switch S1 reveals that interfaces F0/1 and F0/3 only allow VLANs 10 and 99. Someone updated the documentation but forgot to reconfigure the ports on the S1 switch.

Example 3-19 Missing VLANs

```
S3# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/3       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/3       10,20,99

Port        Vlans allowed and active in management domain
Fa0/3       10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,20,99
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99
Fa0/3       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99
Fa0/3       10,99
<output omitted>
```

Reconfigure F0/1 and F0/3 on switch S1 using the switchport trunk allowed vlan 10,20,99 command, as shown in Example 3-20. The output shows that VLANs 10, 20, and 99 are now added to the F0/1 and F0/3 ports on switch S1. The show interfaces trunk command is an excellent tool for revealing common trunking problems. PC5 has regained connectivity to the student email server found at IP address 172.17.20.10

Example 3-20 Corrected VLAN List

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# interface f0/3
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# end
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99
Fa0/3       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,99
Fa0/3       10,20,99
<output omitted>
PC5> ping 172.17.20.10
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
<output omitted>
```

Packet Tracer Activity 3.2.4.7: Troubleshooting a VLAN Implementation–Scenario 1

In this activity, you will troubleshoot connectivity problems between PCs on the same VLAN. The activity is complete when PCs on the same VLAN can ping each other. Any solution you implement must conform to the addressing table.

Packet Tracer Activity 3.2.4.8: Troubleshooting a VLAN Implementation–Scenario 2

In this activity, you will troubleshoot a misconfigured VLAN environment. The initial network has errors. Your objective is to locate and correct the errors in the configurations and establish end-to-end connectivity. Your final configuration should match the topology diagram and addressing table. The native VLAN for this topology is VLAN 56.

Lab 3.2.4.9: Troubleshooting VLAN Configurations

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Troubleshoot VLAN 10
- Part 3: Troubleshoot VLAN 20

VLAN Security and Design (3.3)

The proliferation of network security certifications indicates that the importance of network security is growing. Every configuration, monitoring, maintenance, and troubleshooting procedure in a switched network must include an analysis of the security implications. VLANs and VLAN technologies play an integral role in the design and implementation of switched networks.

Attacks on VLANs (3.3.1)

A number of attacks are specific to the VLAN infrastructure. In this section, the various types of attacks involving VLANs are explored.

Switch Spoofing Attack (3.3.1.1)

There are a number of different types of VLAN attacks in modern switched networks. The VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to abuse. It is important to understand the general methodology behind these attacks and the primary approaches to mitigate them.

VLAN hopping enables traffic from one VLAN to be seen by another VLAN. Switch spoofing is a type of VLAN hopping attack that works by taking advantage of an incorrectly configured trunk port. By default, trunk ports have access to all VLANs and pass traffic for multiple VLANs across the same physical link, generally between switches.

Figure 3-21 illustrates a *switch spoofing attack*.

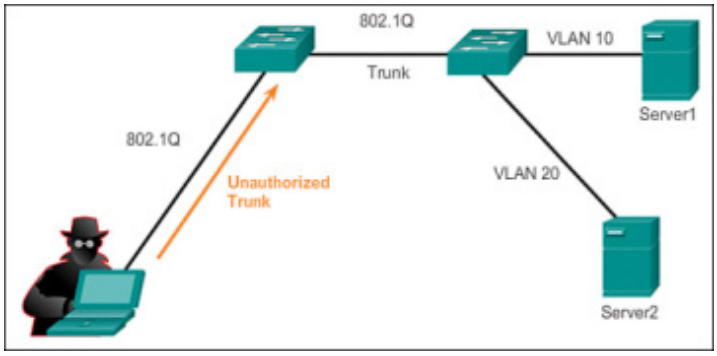

Figure 3-21 Switch Spoofing Attack

In a basic switch spoofing attack, the attacker takes advantage of the fact that the default configuration of the switch port is dynamic auto. The network attacker configures a system to spoof itself as a switch. This spoofing requires that the network attacker be capable of emulating 802.1Q and DTP messages. By tricking a switch into thinking that another switch is attempting to form a trunk, an attacker can gain access to all the VLANs allowed on the trunk port.

The best way to prevent a basic switch spoofing attack is to turn off trunking on all ports, except the ones that specifically require trunking. On the required trunking ports, disable DTP and manually enable trunking.

Double-Tagging Attack (3.3.1.2)

Another type of VLAN attack is a double-tagging (or double-encapsulated) VLAN hopping attack. This type of attack takes advantage of the way that hardware on most switches operates. Most switches perform only one level of 802.1Q deencapsulation, which allows an attacker to embed a hidden 802.1Q tag inside the frame. This tag allows the frame to be forwarded to a VLAN that the original 802.1Q tag did not specify. An important characteristic of the double-encapsulated VLAN hopping attack is that it works even if trunk ports are disabled, because a host typically sends a frame on a segment that is not a trunk link.

A ***double-tagging attack***, illustrated in Figure 3-22, follows three steps:

1. The attacker sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the attacker, which is the same as the native VLAN of the trunk port. The assumption is that the switch processes the frame received from the attacker as if it were on a trunk port or a port with a voice VLAN (a switch should not receive a tagged Ethernet frame on an access port). For the purposes of this example, assume that the native VLAN is VLAN 10. The inner tag is the victim VLAN, in this case, VLAN 20.
2. The frame arrives on the switch, which looks at the first 4-byte 802.1Q tag. The switch sees that the frame is destined for VLAN 10, which is the native VLAN. The switch forwards the packet out on all VLAN 10 ports after stripping the VLAN 10 tag. On the trunk port, the VLAN 10 tag is stripped, and the packet is not retagged because it is part of the native VLAN. At this point, the VLAN 20 tag is still intact and has not been inspected by the first switch.
3. The second switch looks only at the inner 802.1Q tag that the attacker sent and sees that the frame is destined for VLAN 20, the target VLAN. The second switch sends the frame on to the victim port or floods it, depending on whether there is an existing MAC address table entry for the victim host.

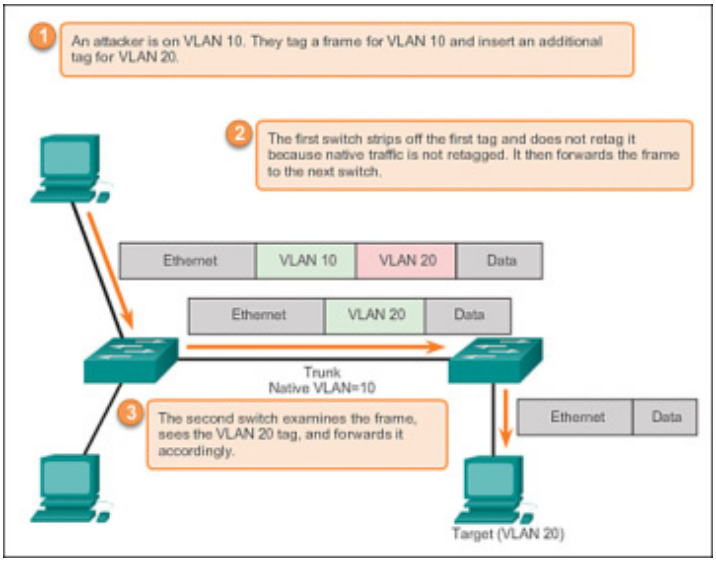

Figure 3-22 Double-Tagging Attack

This type of attack is unidirectional and works only when the attacker is connected to a port residing in the same VLAN as the native VLAN of the trunk port. Thwarting this type of attack is not as easy as stopping basic VLAN hopping attacks.

The best approach to mitigating double-tagging attacks is to ensure that the native VLAN of the trunk ports is different from the VLAN of any user ports. In fact, it is considered a security best practice to use a fixed VLAN that is distinct from all user VLANs in the switched network as the native VLAN for all 802.1Q trunks.

PVLAN Edge (3.3.1.3)

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of the ***Private VLAN (PVLAN) Edge*** feature, also known as ***protected ports***, ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch, as shown in Figure 3-23.

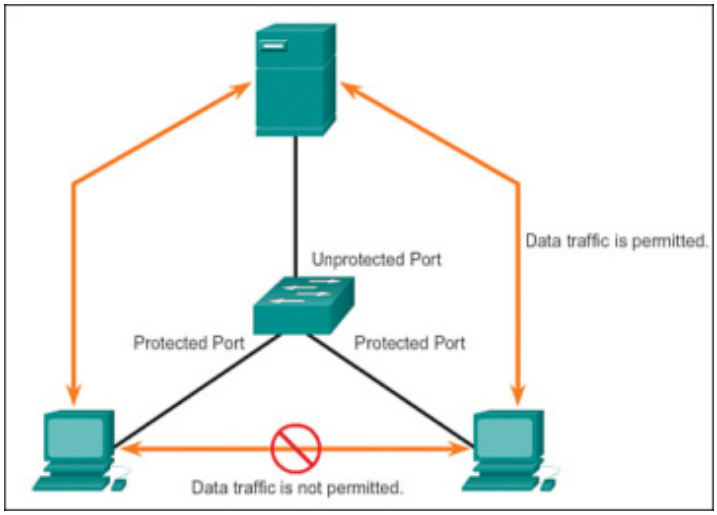

Figure 3-23 Private VLAN Edge

The PVLAN Edge feature has the following characteristics:

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port, except for control traffic. Data traffic cannot be forwarded between protected ports at Layer 2.

- Forwarding behavior between a protected port and a nonprotected port proceeds as usual.
- Protected ports must be manually configured.

To configure the PVLAN Edge feature, enter the **switchport protected** command in interface configuration mode, as shown in Example 3-21. To disable protected port, use the **no switchport protected** interface configuration mode command. To verify the configuration of the PVLAN Edge feature, use the **show interfaces** *interface-id* **switchport** global configuration mode command.

Example 3-21 PVLAN Edge

```
S1(config)# interface g0/1
S1(config-if)# switchport protected
S1(config-if)# end
S1# show interfaces g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>
Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Activity 3.3.1.3: PVLAN Edge

Go to the online course to use the Syntax Checker in the third graphic to configure the PVLAN Edge feature on interface G0/1 and verify the configuration.

Activity 3.3.1.4: Identify the Type of VLAN Attacks

Go to the online course to perform this practice activity.

VLAN Best Practices (3.3.2)

VLAN best practices refer to those practices that any network administrator responsible for portions of a switched network should employ in his day-to-day work. These comprise standard operating procedures for switch practitioners.

VLAN Design Guidelines (3.3.2.1)

Cisco switches have a factory configuration in which default VLANs are preconfigured to support various media and protocol types. The default Ethernet VLAN is VLAN 1. It is a security best practice to configure all the ports on all switches to be associated with VLANs other than VLAN 1. This is usually done by configuring all unused ports to a ***black hole VLAN*** that is not used for anything on the network. All used ports are associated with VLANs distinct from VLAN 1 and distinct from the black hole VLAN. It is also a good practice to shut down unused switch ports to prevent unauthorized access.

A good security practice is to separate management and user data traffic. The management VLAN, which is VLAN 1 by default, should be changed to a separate, distinct VLAN. To communicate remotely with a Cisco switch for management purposes, the switch must have an IP address configured on the management VLAN. Users in other VLANs would not be able to establish remote access sessions to the switch unless they were routed into the management VLAN, providing an additional layer of security. Also, the switch should be configured to accept only encrypted SSH sessions for remote management.

All control traffic is sent on VLAN 1. Therefore, when the native VLAN is changed to something other than VLAN 1, all control traffic is tagged on IEEE 802.1Q VLAN trunks (tagged with VLAN ID 1). A recommended security practice is to change the native VLAN to a different VLAN than VLAN 1. The native VLAN should also be distinct from all user VLANs. Ensure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link.

DTP offers four switch port modes: access, trunk, dynamic auto, and dynamic desirable. A general guideline is to disable autonegotiation. As a port security best practice, do not use the dynamic auto or dynamic desirable switch port modes.

Finally, voice traffic has stringent QoS requirements. If user PCs and IP phones are on the same VLAN, each tries to use the available bandwidth without considering the other device. To avoid this conflict, it is good practice to use separate VLANs for IP telephony and data traffic.

Lab 3.2.4.9: Troubleshooting VLAN Configurations

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Implement VLAN Security on the Switches

Summary (3.4)

Class Activity 3.4.1.1: VLAN Plan

You are designing a VLAN switched network for your small- to medium-sized business.

Your business owns space on two floors of a high-rise building. The following elements need VLAN consideration and access for planning purposes:

- Management
- Finance
- Sales
- Human Resources
- Network administrator
- General visitors to your business location

You have two Cisco 3560-24PS switches.

Use a word processing software program to design your VLAN-switched network scheme.

Section 1 of your design should include the regular names of your departments, suggested VLAN names and numbers, and which switch ports would be assigned to each VLAN.

Section 2 of your design should list how security would be planned for this switched network.

When your VLAN plan is finished, complete the reflection questions from this activity's PDF.

Save your work. Be able to explain and discuss your VLAN design with another group or with the class.

Packet Tracer Activity 3.4.1.2: Skills Integration Challenge

In this activity, two switches are completely configured. On a third switch, you are responsible for assigning IP addressing to the SVI, configuring VLANs, assigning VLANs to interfaces, configuring trunking, and performing basic switch security.

This chapter introduced VLANs. VLANs are based on logical connections, instead of physical connections. VLANs are a mechanism to allow network administrators to create logical broadcast domains that can span across a single switch or multiple switches, regardless of physical proximity. This function is useful to reduce the size of broadcast domains or to allow groups of users to be logically grouped without the need to be physically located in the same place.

There are several types of VLANs:

- Default VLAN
- Management VLAN
- Native VLAN
- User/Data VLANs
- Black Hole VLAN
- Voice VLAN

On a Cisco switch, VLAN 1 is the default Ethernet VLAN, the default native VLAN, and the default management VLAN. Best practices suggest that the native and management VLANs be moved to another distinct VLAN and that unused switch ports be moved to a "black hole" VLAN for increased security.

The **switchport access vlan** command is used to create a VLAN on a switch. After creating a VLAN, the next step is to assign ports to the VLAN. The **show vlan brief** command displays the VLAN assignment and membership type for all switch ports. Each VLAN must correspond to a unique IP subnet.

Use the **show vlan** command to check whether the port belongs to the expected VLAN. If the port is assigned to the wrong VLAN, use the **switchport access vlan** command to correct the VLAN membership. Use the **show mac address-table** command to check which addresses were learned on a particular port of the switch and to which VLAN that port is assigned.

A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs.

VLAN trunks facilitate inter-switch communication by carrying traffic associated with multiple VLANs. IEEE 802.1Q frame tagging differentiates between Ethernet frames associated with distinct VLANs as they traverse common trunk links. To enable trunk links, use the **switchport mode trunk** command. Use the **show interfaces trunk** command to check whether a trunk has been established between switches.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis only, between network devices. DTP is a Cisco-proprietary protocol that is automatically enabled on Catalyst 2960 and Catalyst 3560 Series switches.

To place a switch into its factory default condition with one default VLAN, use the **delete flash:vlan.dat** and **erase startup-config** commands.

This chapter also examined the configuration, verification, and troubleshooting of VLANs and trunks using the Cisco IOS CLI and explored basic security and design considerations in the context of VLANs.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Switched Networks Lab Manual* (ISBN 978-1-58713-372-5). The Packet Tracer Activities PKA files are found in the online course.

Class Activities

- Class Activity 3.0.1.2: Vacation Station
- Class Activity 3.4.1.1: VLAN Plan

Labs

- Lab 3.2.2.5: Configuring VLANs and Trunking
- Lab 3.2.4.9: Troubleshooting VLAN Configurations

Packet Tracer Activities

- Packet Tracer Activity 3.1.1.5: Who Hears the Broadcast?
- Packet Tracer Activity 3.1.2.7: Investigating a VLAN Implementation
- Packet Tracer Activity 3.2.1.7: Configuring VLANs
- Packet Tracer Activity 3.2.2.4: Configuring Trunks
- Packet Tracer Activity 3.2.4.7: Troubleshooting a VLAN Implementation—Scenario 1
- Packet Tracer Activity 3.2.4.8: Troubleshooting a VLAN Implementation—Scenario 2

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix “Answers to ‘Check Your Understanding’ Questions” lists the answers.

1. For what reason would a network administrator use the **show interfaces trunk** command on a switch?

   A. To view the native VLAN
   B. To examine DTP negotiation as it occurs
   C. To verify port association with a particular VLAN
   D. To display an IP address for any existing VLAN

2. What is the purpose of the switch command **switchport access vlan 99**?

   A. To enable port security
   B. To make the port operational
   C. To assign the port to a particular VLAN
   D. To designate the VLAN that does not get tagged
   E. To assign the port to the default native VLAN (VLAN 99)

3. Which step should be performed first when deleting a VLAN that has member switch ports?

A. Reload the switch.
B. Implement the **delete vlan.dat** command.
C. Reassign all VLAN member ports to a different VLAN.
D. Back up the running config.

4. All access ports on a switch are configured with the administrative mode of dynamic auto. An attacker, connected to one of the ports, sends a malicious DTP frame. What is the intent of the attacker?

   A. VLAN hopping attack
   B. DHCP spoofing attack
   C. MAC flooding attack
   D. ARP poisoning attack

5. Which of the following statements accurately describe DTP? (Choose two.)

   A. DTP is a Cisco-proprietary protocol.
   B. DTP supports IEEE 802.1Q.
   C. Cisco switches require DTP to establish trunks.
   D. DTP must be enabled on only one side of the trunk link.
   E. Trunk ports that are configured for dynamic auto will request to enter the trunking state.

6. Match the action to the corresponding command.

   A. Assigns VLAN 10 for untagged traffic
   B. Activates the current interface as trunk
   C. Prohibits VLAN 10 on the trunk interface
   D. Switch(config-if)# **switchport trunk allowed vlan remove 10**
   E. Switch(config-if)# **switchport mode trunk**
   F. Switch(config-if)# **switchport trunk native vlan 10**

7. What is one way to prevent the VLAN hopping attack?

   A. Disable DTP negotiation on all ports.
   B. Change the native VLAN to an unused VLAN.
   C. Designate a different default VLAN.
   D. Remove all user VLANs from the trunk.

8. What security issue is of concern regarding the VLAN configuration of switches?

   A. All interfaces are in the same user VLAN.
   B. The management VLAN is using the same VLAN ID as a user VLAN is using.
   C. The “black hole” VLAN is not configured.
   D. The native VLAN has not been changed from the default setting.

9. In which location are the normal-range VLANs stored on a Cisco switch by default?

   A. Flash memory
   B. Startup config
   C. Running config
   D. RAM

10. Which of the following statements describe the benefits of VLANs? (Choose two.)

    A. VLANs improve network performance by regulating flow control and window size.
    B. VLANs enable switches to route packets to remote networks through VLAN ID filtering.
    C. VLANs reduce network cost by reducing the number of physical ports required on switches.
    D. VLANs improve network security by isolating users that have access to sensitive data and applications.
    E. VLANs divide a network into smaller logical networks, resulting in lower susceptibility to broadcast storms.

11. An administrator is investigating an inoperational trunk link between a Cisco switch and a switch from another vendor. After a few **show** commands, the

administrator notices that the switches are not negotiating a trunk. What is a probable cause for this issue?

A. Both switches are in trunk mode.
B. Both switches are in nonegotiate mode.
C. Switches from other vendors do not support DTP.
D. DTP frames are flooding the entire network.

12. Which distinct type of VLAN is used by an administrator to access and configure a switch?

A. Default VLAN
B. Native VLAN
C. Data VLAN
D. Management VLAN
