CHAPTER 3

VLANs

Objectives

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

- What is the role of a VLAN in a switched LAN?
- What is the role of a VLAN trunk in a switched LAN?
- How do you configured VLANs on switches in a switched LAN?
- How do you troubleshoot common software and hardware configuration problems associated with VLANs in a switched LAN?

Key Terms

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

vlan.dat *page 126*

Flash *page 126*

VLAN trunking protocol (VTP) *page 126*

data VLAN *page 127*

default VLAN *page 128*

black hole VLAN *page 128*

native VLAN *page 129*

IEEE 802.1Q *page 129*

management VLAN *page 130*

voice VLAN *page 131*

signaling traffic *page 133*

Static VLAN *page 137*

Dynamic VLAN *page 137*

switch virtual interface (SVI) *page 141*

VLAN trunk *page 144*

IEEE 802.1p *page 146*

Canonical Format Identifier (CFI) *page 146*

VLAN ID (VID) *page 146*

untagged frames *page 147*

inter-switch link (ISL) *page 149*

Dynamic Trunking Protocol (DTP) *page 149*

trunking modes *page 149*

nonegotiate *page 150*

dynamic auto *page 150*

dynamic desirable *page 151*

allowed VLANs *page 163*

Network performance can be a factor in an organization's productivity and its reputation for delivering as promised. One of the technologies contributing to excellent network performance is the separation of large broadcast domains into smaller ones with VLANs. Smaller broadcast domains limit the number of devices participating in broadcasts and allow devices to be separated into functional groups, such as database services for an accounting department and high-speed data transfer for an engineering department. In this chapter, you learn how to configure, manage, and troubleshoot VLANs and Ethernet trunk links.

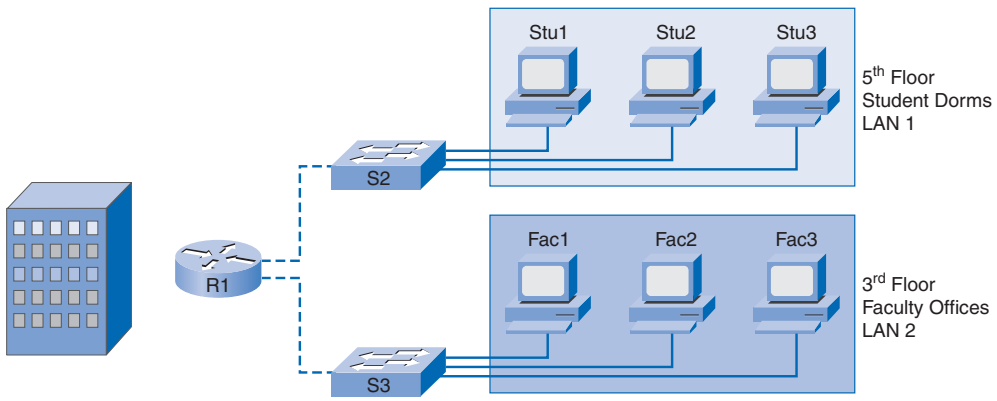
Introducing VLANs

Switches and VLANs go together—you cannot have one without the other. Although it is possible to configure a modern switch to have only one VLAN, normally a switch will have two or more VLANs. VLANs give network administrators flexibility in LAN design. VLANs extend the traditional router-bounded broadcast domain to a VLAN-bounded broadcast domain; VLANs make it possible to sculpt a broadcast domain into any shape that can be defined and bounded by the switches within the network. In this section, you learn what the different types of VLANs are and how to configure them and extend them using Ethernet trunks. First you explore the historical implementation of VLANs versus the modern implementation.

Defining VLANs

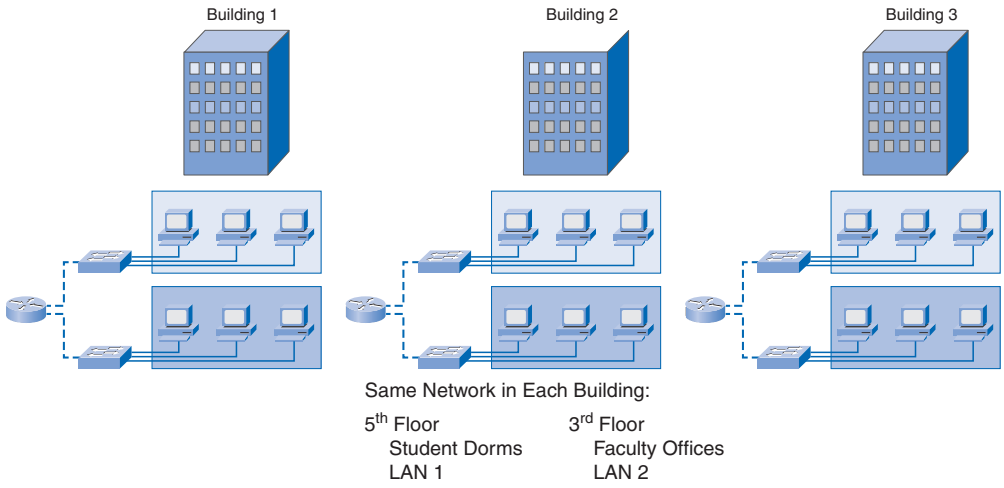
To appreciate why VLANs are being widely used today, consider a small university with student dorms and faculty offices all in one building. Figure 3-1 shows the student computers in one LAN and the faculty computers in another LAN. This works fine because each department is physically together, so it is easy to provide them with their network resources.

Figure 3-1 Before VLANs—One Building



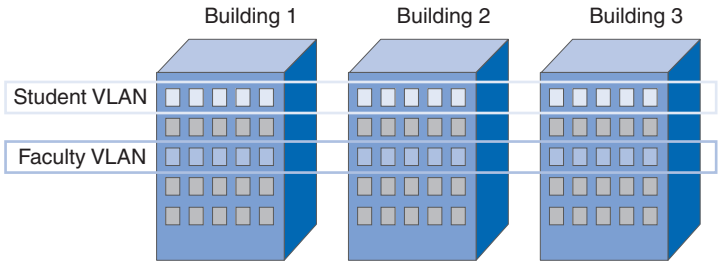
A year later, the university has grown and now has three buildings. In Figure 3-2, the original network is the same, but student and faculty computers are spread out across three buildings. The student dorms remain on the fifth floor and the faculty offices remain on the third floor. However, now the IT department wants to ensure that student computers all share the same security features and bandwidth controls. How can the network accommodate the shared needs of the geographically separated departments? Do you create a large LAN and wire each department together? How easy would it be to make changes to that network? It would be nice to be able to group the people with the resources they use regardless of their geographic location, and it would make it easier to manage their specific security and bandwidth requirements.

Figure 3-2 Before VLANs—Three Buildings



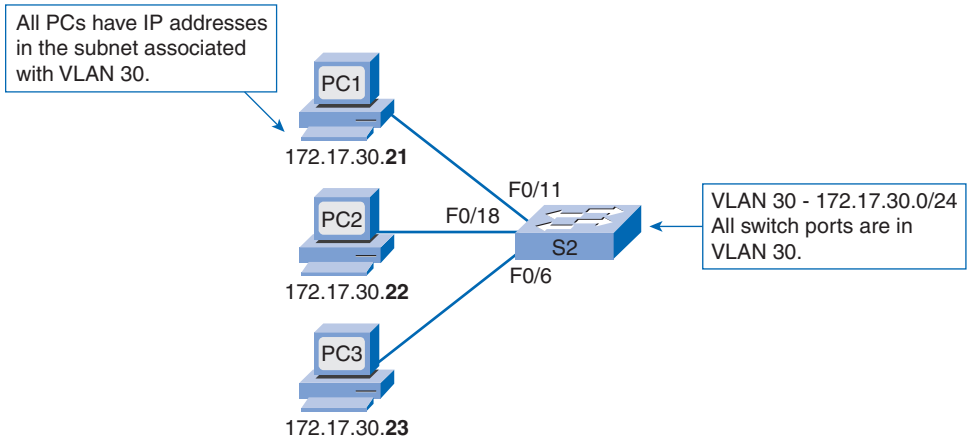
The solution for the university is to use a networking technology called a virtual LAN (VLAN). A VLAN allows a network administrator to create groups of logically networked devices that act as if they are on their own independent network, even if they share a common infrastructure with other VLANs. When you configure a VLAN, you can name it to describe the primary role of the users for that VLAN. As another example, all the student computers in a university can be configured in the "Student" VLAN. Using VLANs, you can logically segment switched networks based on functions, departments, or project teams. You can also use a VLAN to geographically structure your network to support the growing reliance of companies on home-based workers. In Figure 3-3, one VLAN is created for students and another for faculty. These VLANs allow the network administrator to implement access and security policies to particular groups of users. For example, the faculty, but not the students, can be allowed access to e-learning management servers for developing online course materials.

Figure 3-3 After VLANs—Three Buildings



A VLAN is a logically separate IP subnetwork. VLANs allow multiple IP networks and subnets to exist on the same switched network. Figure 3-4 shows a network with three computers. For computers to communicate on the same VLAN, each must have an IP address and a subnet mask that is consistent for that VLAN. The switch has to be configured with the VLAN, and each port in the VLAN must be assigned to the VLAN. A switch port with a singular VLAN configured on it is called an access port. Remember that just because two computers are physically connected to the same switch does not mean that they can communicate. Devices on two separate subnets must communicate via a router (Layer 3), whether or not VLANs are used. You do not need VLANs to have multiple subnets on a switched network, but definite advantages exist to using VLANs.

Figure 3-4 Switches Define VLANs

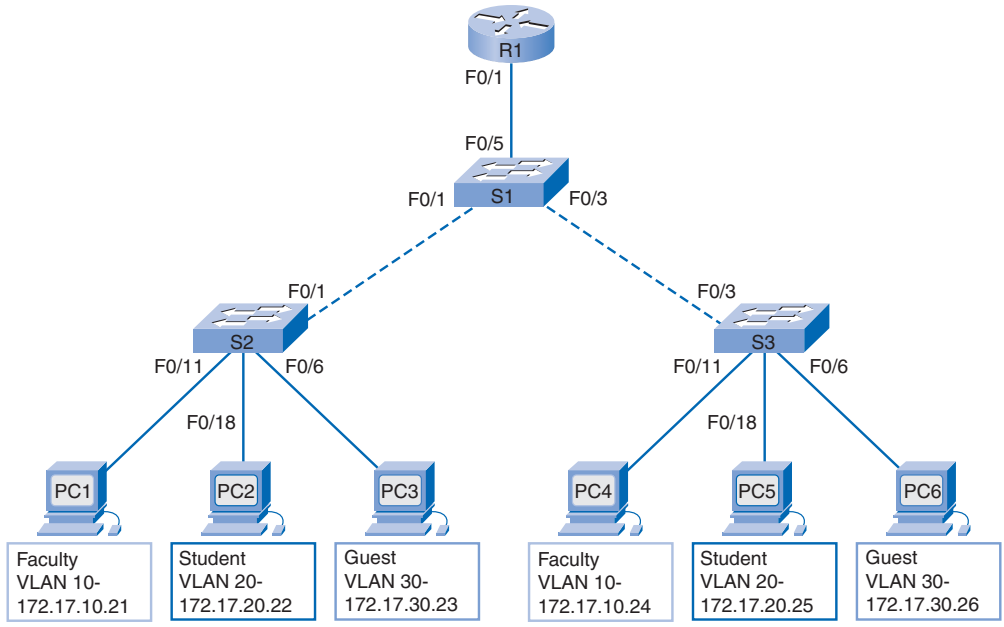


Benefits of VLANs

User productivity and network adaptability are key drivers for business growth and success. Implementing VLAN technology enables a network to more flexibly support business goals. The primary benefits of using VLANs are the following:

- **Security:** Groups that have sensitive data are separated from the rest of the network, decreasing the chances of confidential information breaches. Faculty computers are on VLAN 10 and completely separated from student and guest data traffic.
- **Cost reduction:** Cost savings result from less need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.
- **Higher performance:** Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces unnecessary traffic on the network and boosts performance.
- **Broadcast storm mitigation:** Dividing a network into VLANs reduces the number of devices that may participate in a broadcast storm. LAN segmentation prevents a broadcast storm from propagating throughout the entire network. In Figure 3-5, you can see 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 you provision a new switch, 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 3-5, for easy identification VLAN 10 is Faculty, VLAN 20 is Student, and VLAN 30 is Guest.

Figure 3-5 Naming VLANs



- **Simpler project or 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—for example, e-learning development software for faculty. VLANs also ease the determination of the effects of upgrading network services.

VLAN ID Ranges

VLANs are divided numerically into a normal range and an extended range. Normal range VLANs are characterized as follows:

- 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. You learn more about VLAN 1 later in this chapter.
- 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 learn only normal range VLANs and stores them in the VLAN database file.

Extended range VLANs are characterized as follows:

- 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.
- Support fewer VLAN features than normal range VLANs.
- Are saved in the running configuration file.
- VTP does not learn extended range VLANs.

One Cisco Catalyst 2960 switch can support up to a combination of 255 VLANs among the collection of both normal and extended range VLANs. The number of VLANs configured affects the performance of the switch hardware. Because an enterprise network may need a switch with a lot of ports, Cisco has developed enterprise-level switches that can be clustered or stacked together to create a single switching unit. For example, nine switches with 48 ports can be clustered to operate as a single switching unit with 432 ports. In this case, the 255 VLAN limit per single switch may be a constraint for some enterprise customers.

Types of VLANs

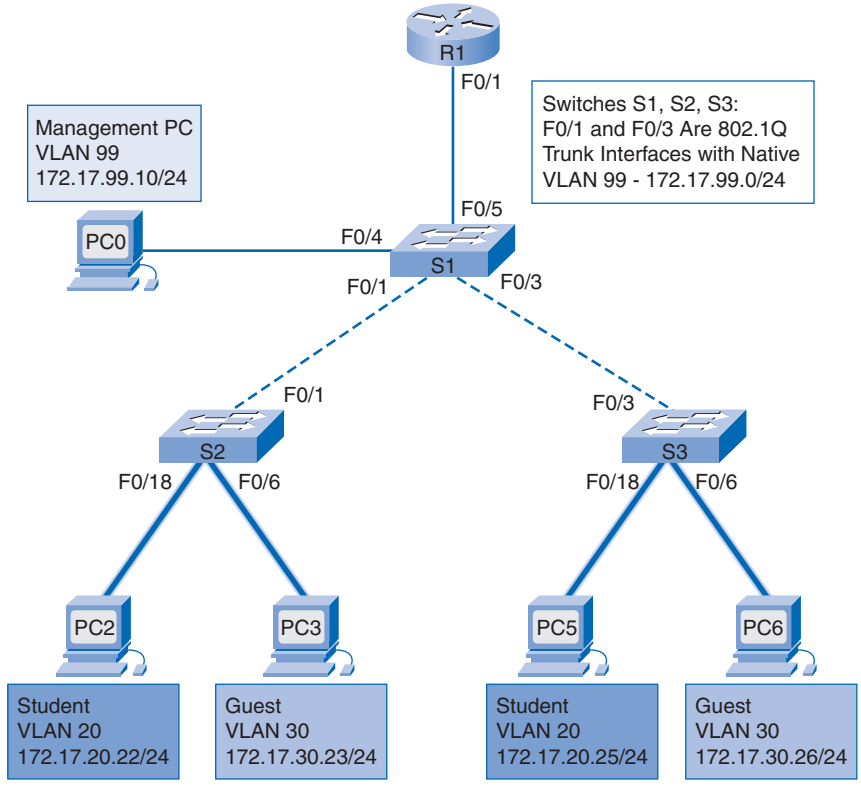
Today there is essentially one way of implementing VLANs: port-based VLANs. With a port-based VLAN, a VLAN is associated with a set of switch ports in the broadcast domain. The ports that are associated with a port-based VLAN are called access ports. In a sense, a VLAN is defined by the access ports assigned to it.

Among the (port-based) VLANs are a number of types of VLANs. Some VLAN types are defined by the type of traffic they support; others are defined by the specific functions they perform. The principal VLAN types are data VLANs, the default VLAN, the black hole VLAN, native VLANs, management VLANs, and voice VLANs.

Because switches will be carrying traffic associated with several VLANs, ports connecting to other switches are used to carry traffic for more than one VLAN; these are called trunk ports. Figure 3-6 shows trunk links between switches. A detailed discussion of trunks is developed in the next section.

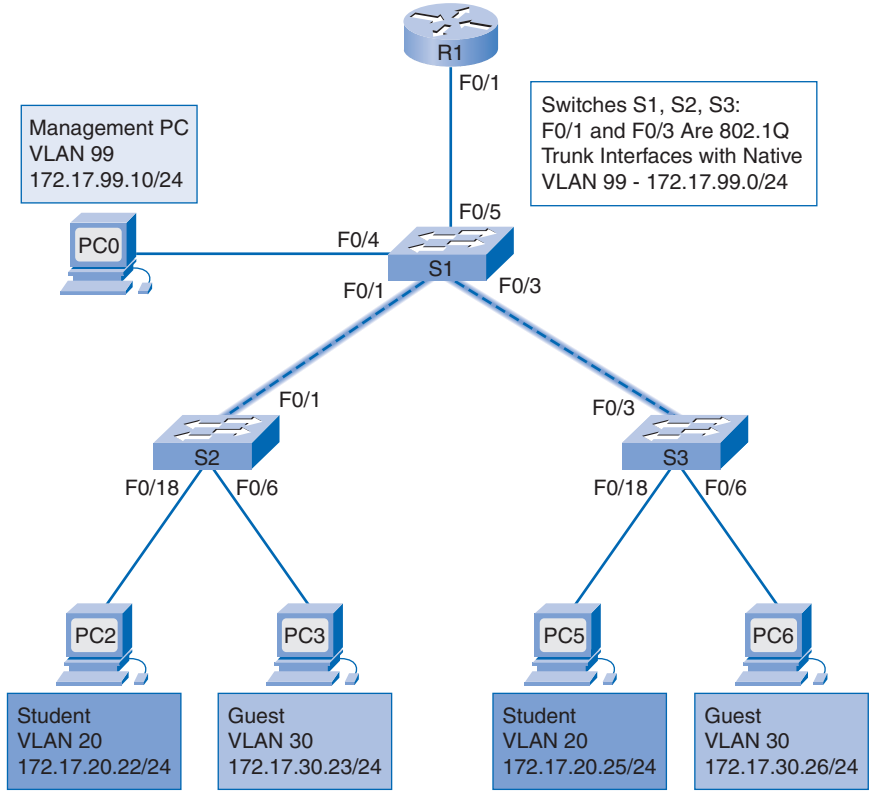
A ***data VLAN*** is a VLAN that is configured to carry only user-generated traffic. Typically, multiple data VLANs populate a switched infrastructure. A VLAN could carry voice-based traffic or traffic used to manage the switch, but this traffic would not be part of a data VLAN. It is common practice to separate voice and management traffic from data traffic. The importance of separating user data from switch management traffic and voice traffic is highlighted by the use of a special term used to identify VLANs that carry only user data—a data VLAN. A data VLAN is sometimes called a user VLAN. Figure 3-6 illustrates the portion of a network covered by user VLANs.

Figure 3-6 Data VLANs



The ***default VLAN*** is the VLAN that all the ports on a switch are members of when a switch is reset to factory defaults. All switch ports are members of the default VLAN after the initial boot of the switch. If all the switch ports are members of the default VLAN, they are all part of the same broadcast domain; this allows any device connected to any switch port to communicate with any device on any other switch port. The default VLAN for Cisco switches is VLAN 1. VLAN 1 has all the features of any VLAN, except that you cannot rename it and you cannot delete it. Layer 2 control traffic, such as CDP and Spanning Tree Protocol traffic, will always be associated with VLAN 1—this cannot be changed. It is a security best practice to restrict VLAN 1 to serve as a conduit only for Layer 2 control traffic, supporting no other traffic. In Figure 3-7, VLAN 1 traffic is forwarded over the VLAN trunks connecting interfaces F0/1 and F0/3 on the S1, S2, and S3 switches. VLAN trunks support the transmission of traffic from more than one VLAN. Although VLAN trunks are mentioned in this section, they are formally introduced in the next section, "VLAN Trunking."

Figure 3-7 VLAN 1—Default VLAN on Catalyst Switches

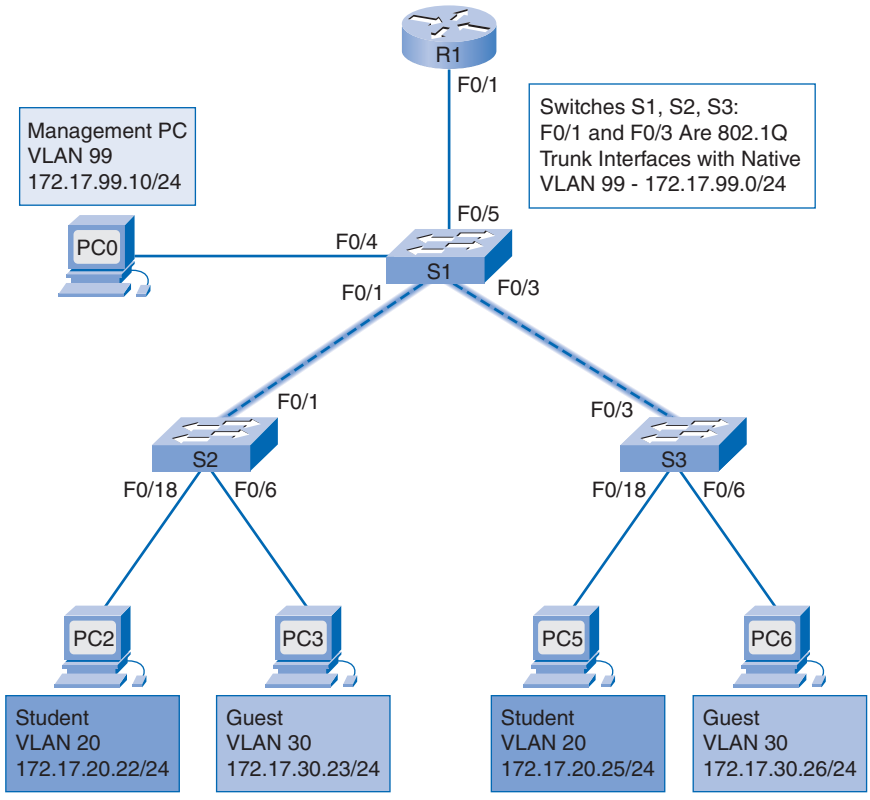


Some network administrators use the term *default VLAN* to mean a VLAN other than VLAN 1 defined by the network administrator as the VLAN that all ports are assigned to when they are not in use. We introduce the term ***black hole VLAN*** to distinguish this VLAN from the default VLAN. The default VLAN is intrinsic to the switch out-of-the-box; it is

VLAN 1 on Cisco switches. The black hole VLAN is defined by the switch administrator. It is a security best practice to define a black hole VLAN to be a dummy VLAN distinct from *all* other VLANs defined in the switched LAN. All unused switch ports are assigned to the black hole VLAN so that any device connecting to an unused switch port will be assigned to the black hole VLAN. Any traffic associated with the black hole VLAN is not allowed on trunk links, thus preventing any device associated with the black hole VLAN from communicating beyond the switch to which it is connected.

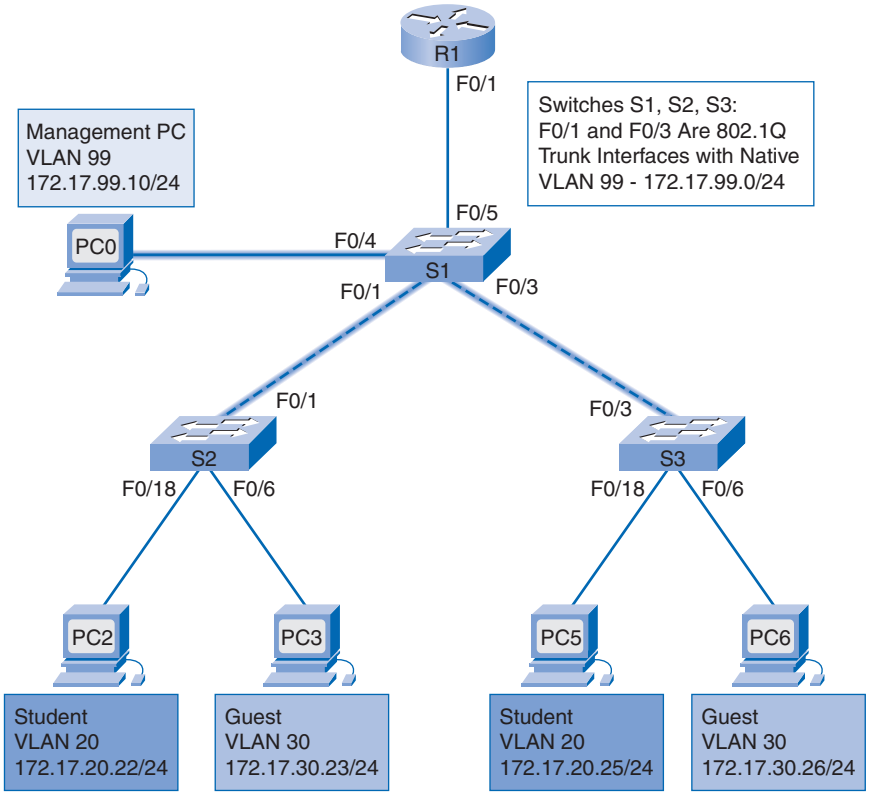
A ***native VLAN*** is assigned to an 802.1Q trunk port. An ***IEEE 802.1Q*** trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. In Figure 3-8, the native VLAN is VLAN 99. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. Native VLANs are set out in the IEEE 802.1Q specification to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For our purposes, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a security best practice to define a native VLAN to be a dummy VLAN distinct from all other VLANs defined in the switched LAN. The native VLAN is not used for any traffic in the switched network unless legacy bridging devices happen to be present in the network, or a multiaccess interconnection exists between switches joined by a hub (not likely in a modern network).

Figure 3-8 Native VLAN



A ***management VLAN*** is a VLAN defined by the switch administrator as a means to access the management capabilities of a switch. VLAN 1 would serve as the management VLAN if you did not proactively define a unique VLAN to serve as the management VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Catalyst switch has VLAN 1 as the default VLAN, you see that VLAN 1 or the black hole VLAN would be a bad choice as the management VLAN; you wouldn't want an arbitrary user connecting to a switch to default to the management VLAN. It is a security best practice to define the management VLAN to be a VLAN distinct from all other VLANs defined in the switched LAN. For simplicity, because of the 24-port limitation of the Catalyst 2960 switches that we reference in Packet Tracer activities, labs, and illustrative examples, for our purposes in this book we use VLAN 99 for both the management VLAN and the native VLAN. A management VLAN is depicted in Figure 3-9.

Figure 3-9 Management VLAN



The one remaining VLAN type, voice VLANs, we explore in the next section.

Voice VLANs

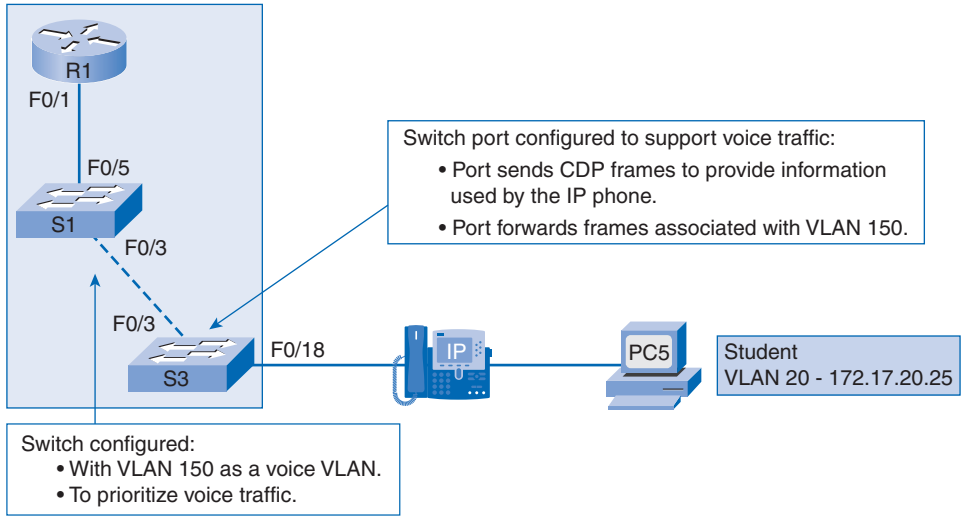
It is easy to appreciate why a separate VLAN is needed to support Voice over IP (VoIP). Imagine that you are receiving an emergency call and suddenly the quality of the transmission degrades so much you cannot understand what the caller is saying. VoIP traffic requires the following:

- 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 milliseconds (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 book, but it is useful to summarize how a ***voice VLAN*** works between a Catalyst switch, a Cisco IP phone, and a computer.

In Figure 3-10, 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. The F0/18 port on S3 is configured as an access port with the voice VLAN feature enabled; as such, the switch uses CDP to instruct the phone to tag voice frames with VLAN 150.

Figure 3-10 Voice VLANs



Note

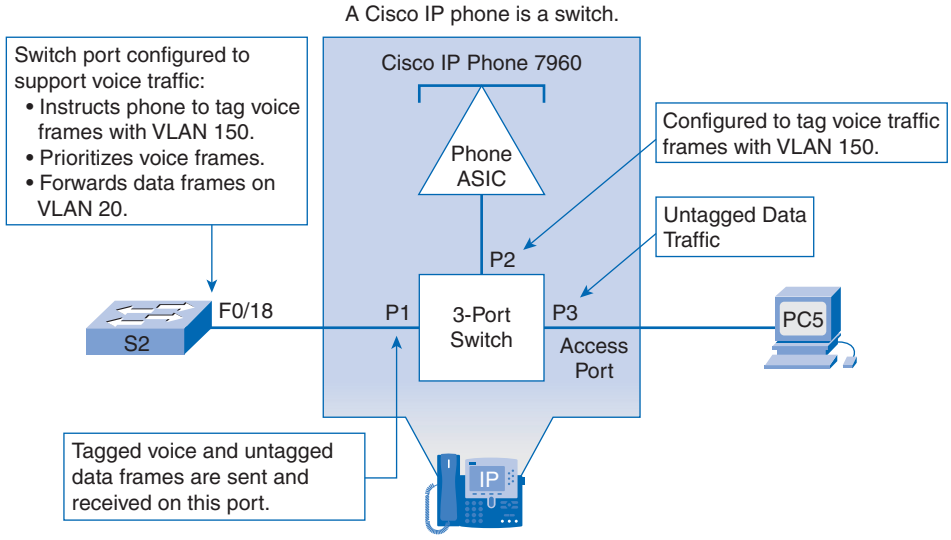
Communication between the switch and IP phone is facilitated by the CDP protocol. This protocol is discussed in greater detail in the *Routing Protocols and Concepts CCNA Exploration Companion Guide*.

Data frames coming through the Cisco IP phone from PC5 are left untagged. Data destined for PC5 coming from port F0/18 is tagged with VLAN 20 on the way to the phone, which strips the VLAN tag before the data is forwarded to PC5. Tagging refers to the addition of VLAN information to a field in the data frame that is used by the switch to identify which VLAN the data frame should be sent to. You learn later about how data frames are tagged.

The Cisco IP phone contains an integrated three-port 10/100 switch, as shown in Figure 3-11. 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.

Figure 3-11 Cisco IP Phone Integrated Switch



The voice VLAN feature enables switch ports to carry IP voice traffic from an IP phone. When the switch is connected to an IP phone, the switch sends CDP messages that instruct the attached IP phone to send voice traffic tagged with the voice VLAN ID 150. The traffic from the PC attached to the IP phone passes through the IP phone untagged. When the switch port has been configured with a voice VLAN, the link between the switch and the IP phone acts as a modified trunk to carry both the tagged voice traffic and untagged data traffic.

Example 3-1 shows sample switch port output associated with an IP phone-connected port.

Example 3-1 Voice VLAN Output

```
S3# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (VLAN0150)
<output omitted>
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

A discussion of the voice-related Cisco IOS commands is beyond the scope of this book, but you can see that 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).

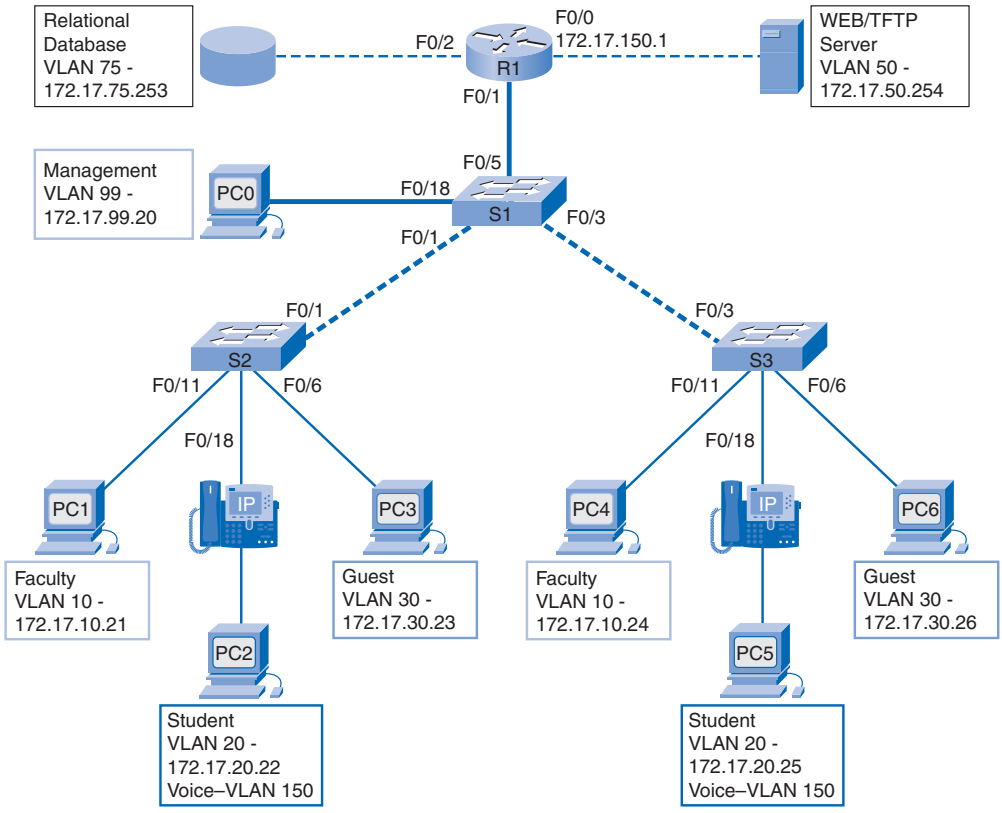
Network Application Traffic Types

In *CCNA Exploration: Network Fundamentals*, you learned about the different kinds of traffic a LAN handles. Because a VLAN has all the characteristics of a LAN, a VLAN must accommodate the same network traffic as a LAN. This includes network management traffic, control traffic, IP telephony traffic, multicast traffic, normal data traffic, and scavenger class traffic.

Many types of network management and control traffic can be present on the network, such as CDP messaging, Simple Network Management Protocol (SNMP) traffic, and Remote Network Monitoring (RMON) traffic. Network management traffic is pictured in Figure 3-12.

IP telephony traffic consists of ***signaling traffic*** and voice traffic. Signaling traffic is responsible for call setup, progress, and teardown. The other type of telephony traffic consists of the actual voice conversation, illustrated in Figure 3-13. As you just learned, in a network configured with VLANs, it is strongly recommended that you assign a VLAN distinct from all other VLANs as the management VLAN. Data traffic should be associated with a data VLAN (other than VLAN 1), and voice traffic should be associated with a voice VLAN.

Figure 3-12 Network Management Traffic



IP multicast traffic is sent from a particular source address to a multicast group that is identified by a single IP address representing a set of receivers configured with that multicast IP address. You learn in multicast theory how multicast MAC addresses are mapped to multicast IP addresses. An example of an application that generates this type of traffic is a Cisco IP/TV broadcast. Multicast traffic can produce a large amount of data streaming across the network. When the network must support multicast traffic, VLANs should be configured to ensure that multicast traffic goes only to those user devices that use the service provided, such as remote video or audio applications. Routers must be configured to ensure that multicast traffic is forwarded strictly to the network areas where it is requested. Figure 3-14 illustrates sample multicast traffic flow.

Normal data traffic is related to file creation and storage, print services, e-mail database access, and other shared network applications that are common to business uses. Figure 3-15 shows sample data traffic flow. VLANs are a natural solution for this type of traffic because you can segment users by their functions or geographic area to more easily manage their specific needs.

Figure 3-13 IP Telephony Traffic

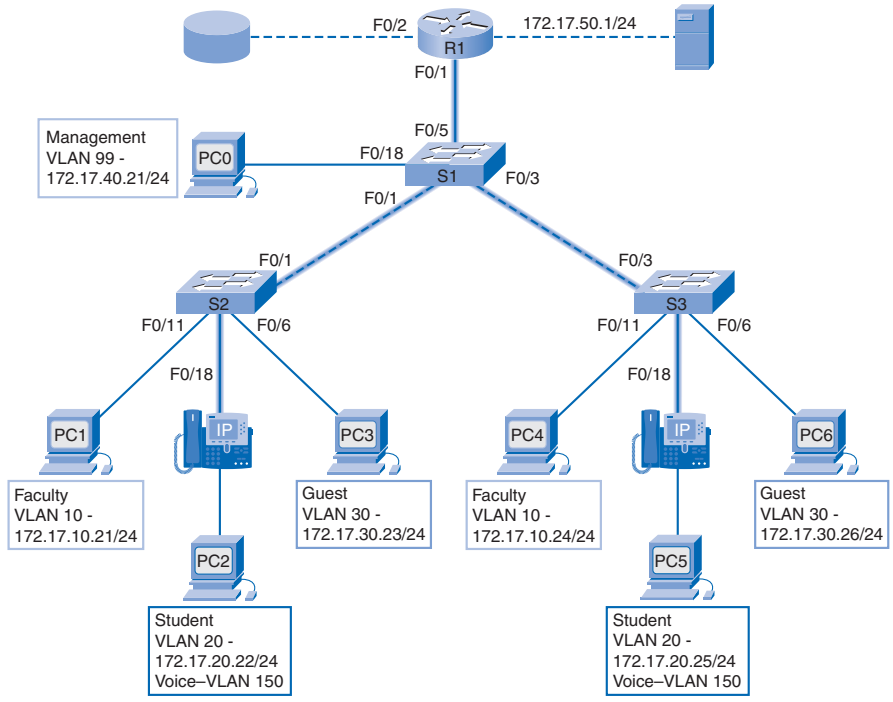


Figure 3-14 IP Multicast Traffic

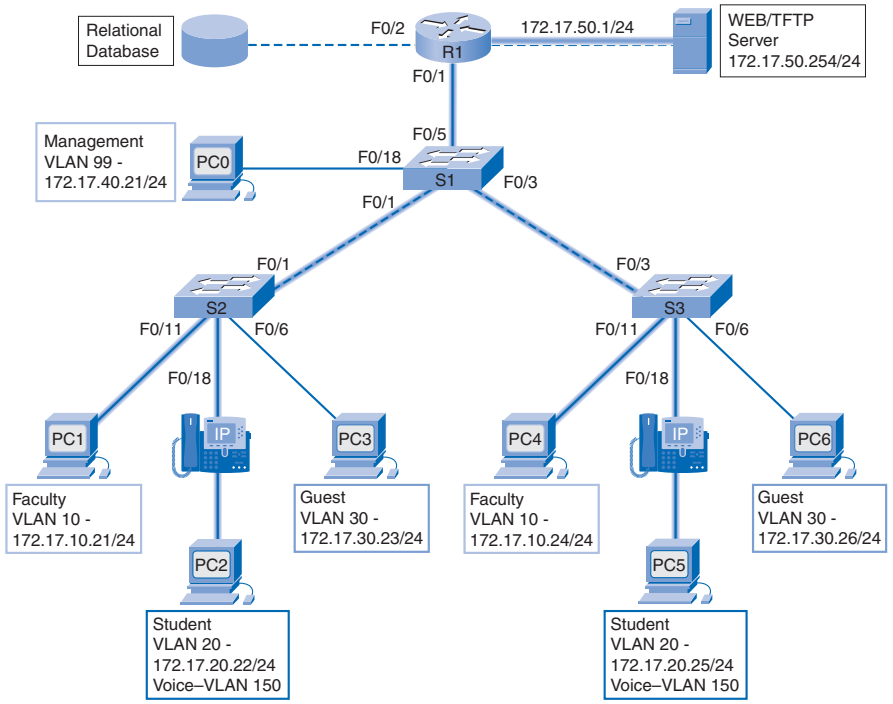
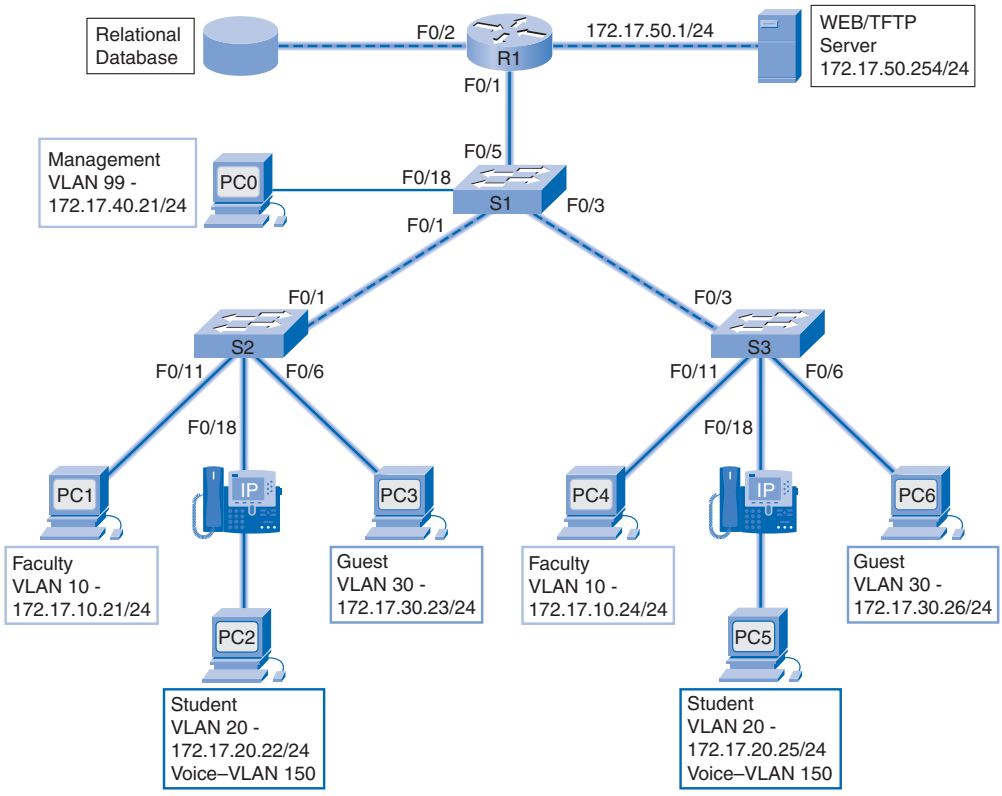


Figure 3-15 Normal Data Traffic



The Scavenger class is intended to provide less-than-best-effort services to certain applications. Applications assigned to this class have little or no contribution to the organizational objectives of the enterprise and are typically entertainment oriented in nature. These include peer-to-peer media-sharing applications (Kazaa, Morpheus, Grokster, Napster, iMesh, and so on), gaming applications (DOOM, Quake, Unreal Tournament, and the like), and any entertainment video applications.

Switch Port Membership Modes

Switch ports are Layer 2 interfaces associated with physical ports. Switch ports are used for managing the physical interfaces and associated Layer 2 protocols. They do not handle routing or bridging. Switch ports belong to one or more VLANs.

When you configure a VLAN, you must assign it a numerical ID, and you can optionally give it a name. The purpose of VLAN implementations is to judiciously associate ports with particular VLANs. You configure the port to forward a frame to a specific VLAN. You can configure a switch port with the voice VLAN feature enabled so as to support both voice and data traffic coming from a Cisco IP phone. You can configure a port to belong to a VLAN by

assigning a membership mode that specifies the kind of traffic the port carries and the VLANs to which it belongs. A port can be configured to support these VLAN options:

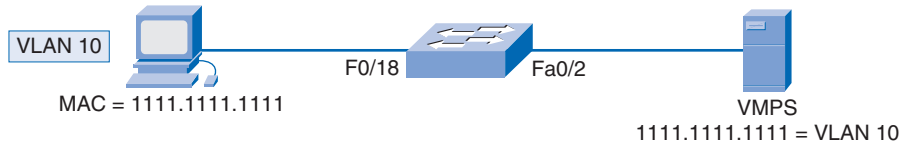
- ***Static VLAN*:** Ports on a switch are manually assigned to a VLAN. Static VLANs are configured using the Cisco CLI. This can also be accomplished with GUI management applications, such as the Cisco Network Assistant. However, a convenient feature of the CLI is that if you assign an interface to a VLAN that does not exist, the new VLAN is created for you. Example 3-2 illustrates a sample static VLAN configuration.

Example 3-2 Static VLAN Configuration

```
S3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)# interface fastEthernet 0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# end
```

- ***Dynamic VLAN***: This option is not widely used in production networks and is not explored in this book. However, it is useful to know what a dynamic VLAN is. Dynamic port VLAN membership is configured using a special server called a VLAN Membership Policy Server (VMPS). With VMPS, you assign switch ports to VLANs dynamically, based on the source MAC address of the device connected to the port. The benefit comes when you move a host from a port on one switch in the network to a port on another switch in the network; the switch dynamically assigns the new port to the proper VLAN for that host. A sample dynamic VLAN implementation is pictured in Figure 3-16.

Figure 3-16 Dynamic VLANs



- **Voice VLAN:** A port is configured with the voice VLAN feature enabled so that it can support an IP phone attached to it. To configure voice support on the port, you need to configure a VLAN for voice and a VLAN for data. In Example 3-3, VLAN 150 is the voice VLAN, and VLAN 20 is the data VLAN. Assume that the network has been configured to ensure that voice traffic can be transmitted with a priority status over the network. When a phone is first plugged into a switch port with voice support enabled, the switch port sends messages to the phone, providing the phone with the appropriate voice VLAN ID and configuration. The IP phone tags the voice frames with the voice VLAN ID and forwards all voice traffic through the voice VLAN.

Example 3-3 Voice VLAN Configuration

```
S3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)# interface fastEthernet 0/18
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# end
S3# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (VLAN0150)
<output omitted>
```

The switch port configuration supporting voice and data has the following characteristics:

- The configuration command **mls qos trust cos** ensures that voice traffic is identified as priority traffic. Remember that the entire network must be set up to prioritize voice traffic. You cannot just configure the port with this command.
- The **switchport voice vlan 150** command identifies VLAN 150 as the voice VLAN. You can see this highlighted in the example: **Voice VLAN: 150 (VLAN0150)**.
- The **switchport access vlan 20** command configures VLAN 20 as the access mode (data) VLAN. You can see this highlighted in the example: **Access Mode VLAN: 20 (VLAN0020)**.

For more details about configuring a voice VLAN, visit this Cisco.com site:

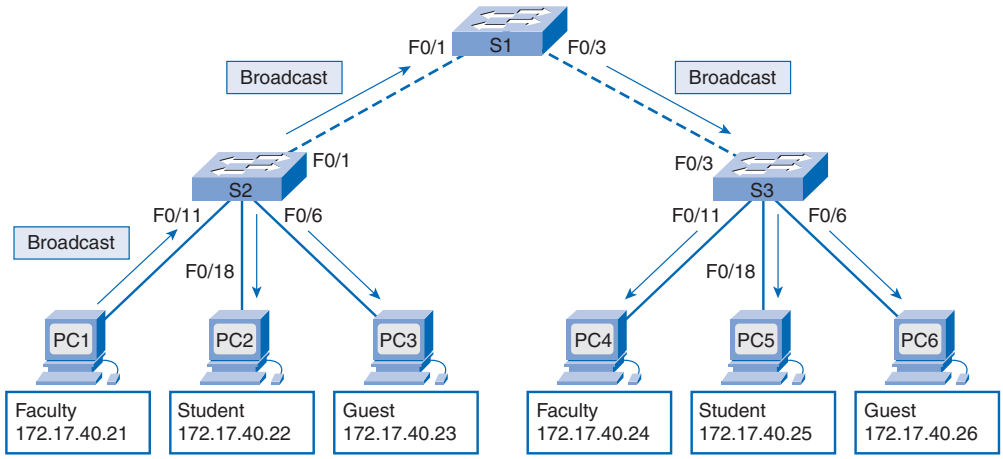
www.cisco.com/en/US/products/ps6406/products_configuration_guide_chapter09186a008081d9a6.html#wp1050913.

Controlling Broadcast Domains with VLANs

In normal operation, when a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports on the switch. In Figure 3-17, the entire network is configured in the same subnet, 172.17.40.0/24. As a result, when the faculty computer, PC1,

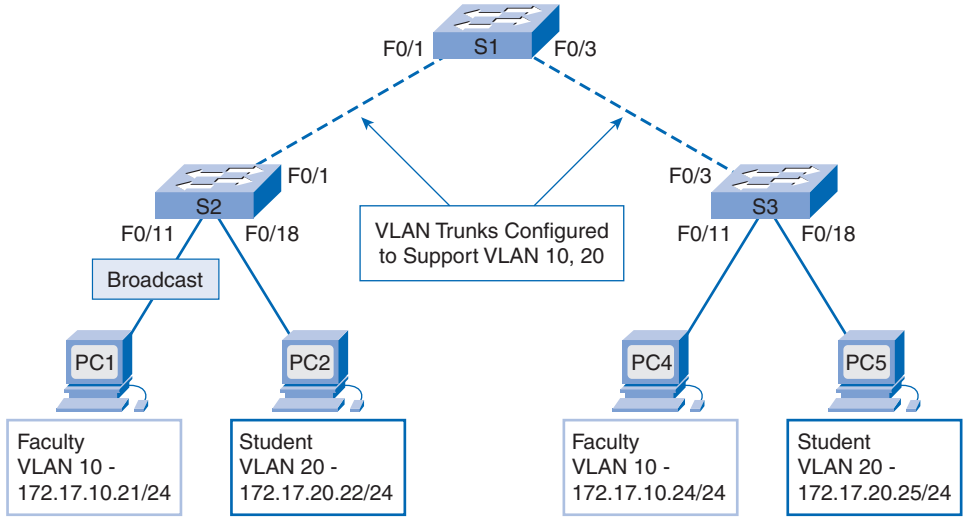
sends out a broadcast frame, switch S2 sends that broadcast frame out all of its ports. Eventually the entire network receives it; the network is one broadcast domain.

Figure 3-17 Single VLAN



In Figure 3-18, the network has been segmented into two VLANs: Faculty as VLAN 10 and Student as VLAN 20. When the broadcast frame is sent from the faculty computer, PC1, to switch S2, the switch forwards that broadcast frame to only those switch ports configured to support VLAN 10. In the figure, the ports that make up the connection between switches S2 and S1 (ports F0/1) and between S1 and S3 (ports F0/3) have been configured to support all the VLANs in the network. This connection is called a *trunk*. You learn more about trunks later in this chapter.

Figure 3-18 Two VLANs



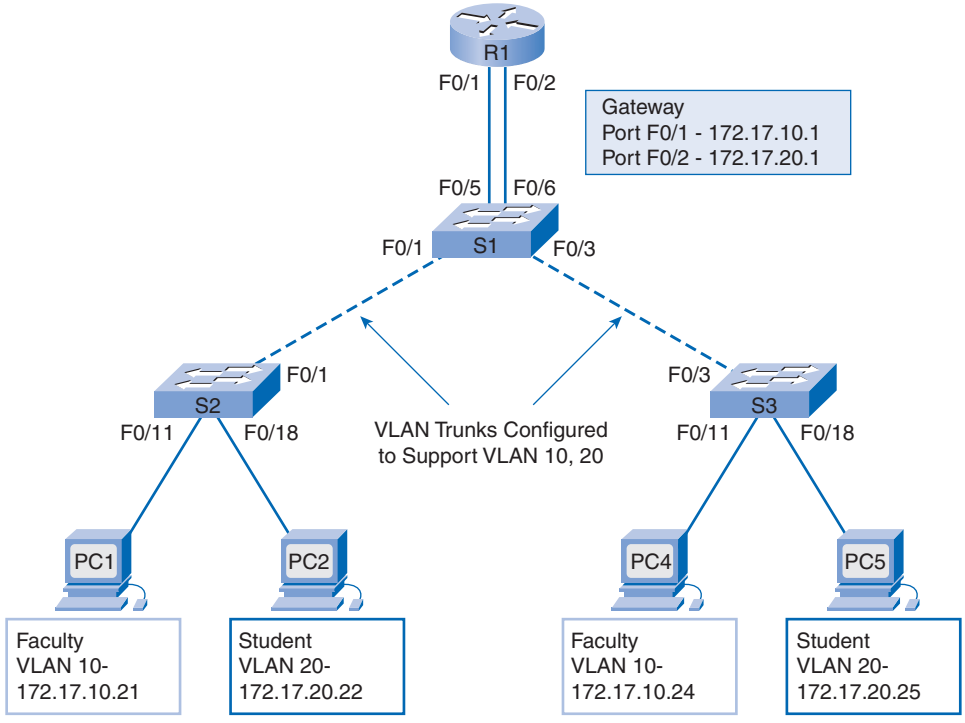
When S1 receives the broadcast frame on port F0/1, S1 forwards that broadcast frame out the only port configured to support VLAN 10, port F0/3. When S3 receives the broadcast frame on port F0/3, it forwards that broadcast frame out the only port configured to support VLAN 10, port F0/11. The broadcast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

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

Breaking up a big broadcast domain into several smaller ones reduces broadcast traffic and improves network performance. Breaking up domains into VLANs also allows for better information confidentiality within an organization. Breaking up broadcast domains can be performed either with VLANs (on switches) or with routers. A router is needed anytime devices on different Layer 3 networks need to communicate, regardless of whether VLANs are used.

In Figure 3-19, PC1 wants to communicate with another device, PC4. PC1 and PC4 are both in VLAN 10.

Figure 3-19 Intra-VLAN Communication



Communicating with a device in the same VLAN is called intra-VLAN communication. The following describes how this process is accomplished:

1. PC1 in VLAN 10 sends an ARP request frame (broadcast) to switch S2. Switch S2 sends the ARP request out port F0/1. Switch S1 sends it out ports F0/5 and F0/3.

Note

There are two connections from switch S1 to the router: one to carry transmissions on VLAN 10 and the other to carry transmissions on VLAN 20 to the router interface.

   Switch S3 sends it out port F0/11 to PC4 on VLAN 10.

2. PC4 sends an ARP reply to switch S3, which forwards it out port F0/3 to switch S1 (router R1 does not reply). Switch S1 forwards the reply out port F0/1. Switch S2 forwards the reply out F0/11. PC1 receives the reply that contains the MAC address of PC4.

3. PC1 now has the destination MAC address of PC4 and uses this to create a unicast frame with PC4's MAC address as the destination. Switches S2, S1, and S3 deliver the frame to PC4.

Again, in Figure 3-19, PC1 in VLAN 10 wants to communicate with PC5 in VLAN 20. Communicating with a device in another VLAN is called inter-VLAN communication.

The following describes how this process is accomplished:

1. PC1 in VLAN 10 wants to communicate with PC5 in VLAN 20. PC1 sends an ARP request frame for the MAC address of the default gateway R1.

2. Router R1 replies with an ARP reply frame from its interface configured on VLAN 10. The reply passes through S1 and S2 and reaches PC1.

3. PC1 then creates an Ethernet frame with the MAC address of the default gateway. The frame is sent through switch S2 and S1 to router R1.

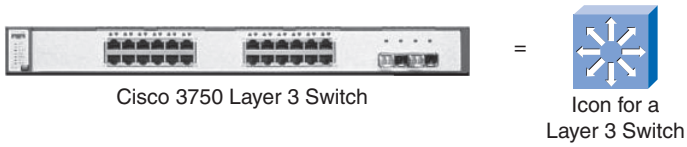
4. Router R1 sends an ARP request frame on VLAN 20 to determine the MAC address of PC5. Switches S1, S2, and S3 broadcast the ARP request frame out ports configured for VLAN 20. PC5 on VLAN 20 receives the ARP request frame from router R1.

5. PC5 on VLAN 20 sends an ARP reply through switches S3 and S1 to router R1 with the destination MAC address of interface F0/2 on router R1.

6. Router R1 sends the frame received from PC1 though S1 and S3 to PC5 (on VLAN 20).

We next explore basic Layer 3 switching. Figure 3-20 shows the Catalyst 3750G-24PS switch, one of many Cisco Catalyst switches that supports Layer 3 switching. The icon that represents a Layer 3 switch is shown. A full discussion of Layer 3 switching is beyond the scope of this book, but a brief description of the ***switch virtual interface (SVI)*** technology that allows a Layer 3 switch to route between VLANs is helpful.

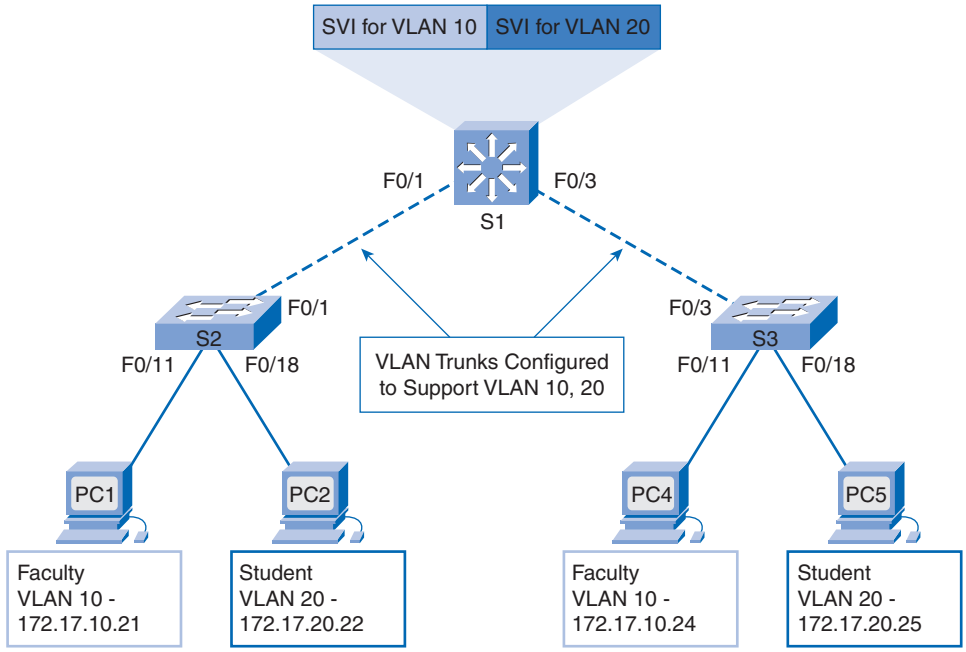
Figure 3-20 Layer 3 Switch



An SVI is a Layer 3 logical interface associated with a specific VLAN. You need to configure an SVI for a VLAN if you want to route between VLANs or to provide IP host connectivity to the switch. By default, an SVI is created for VLAN 1 on a Catalyst switch.

A Layer 3 switch has the capability to route transmissions between VLANs. The procedure is the same as described for the inter-VLAN communication using a separate router, except that the SVIs act as the router interfaces for routing the data between VLANs. Refer to Figure 3-21 for an explanation of the process of inter-VLAN communication via SVIs.

Figure 3-21 Inter-VLAN Communication with SVIs



In the figure, PC1 wants to communicate with PC5. The following steps outline the communication through the Layer 3 switch S1:

1. PC1 sends an ARP request (broadcast) on VLAN10. S2 forwards the ARP request out all ports configured for VLAN 10.

2. Switch S1 forwards the ARP request out all ports configured for VLAN 10, including the SVI for VLAN 10. Switch S3 forwards the ARP request out all ports configured for VLAN 10.
3. Switch S1 knows the location of VLAN 20 because it is a directly connected Layer 3 network in the manner of SVI 20. The SVI for VLAN 10 in switch S1 sends an ARP reply back to PC1 with its MAC address information.
4. PC1 sends data, destined for PC5, as a unicast frame through switch S2 to the SVI for VLAN 10 in switch S1.
5. The SVI for VLAN 20 sends an ARP request broadcast out all switch ports configured for VLAN 20. Switch S3 sends that ARP request broadcast out all switch ports configured for VLAN 20.
6. PC5 on VLAN 20 sends an ARP reply to the SVI for VLAN 20 on S1.
7. The SVI for VLAN 20 forwards the data, sent from PC1, in a unicast frame to PC5 using the destination address it learned from the ARP reply in step 6.

Packet Tracer Activity

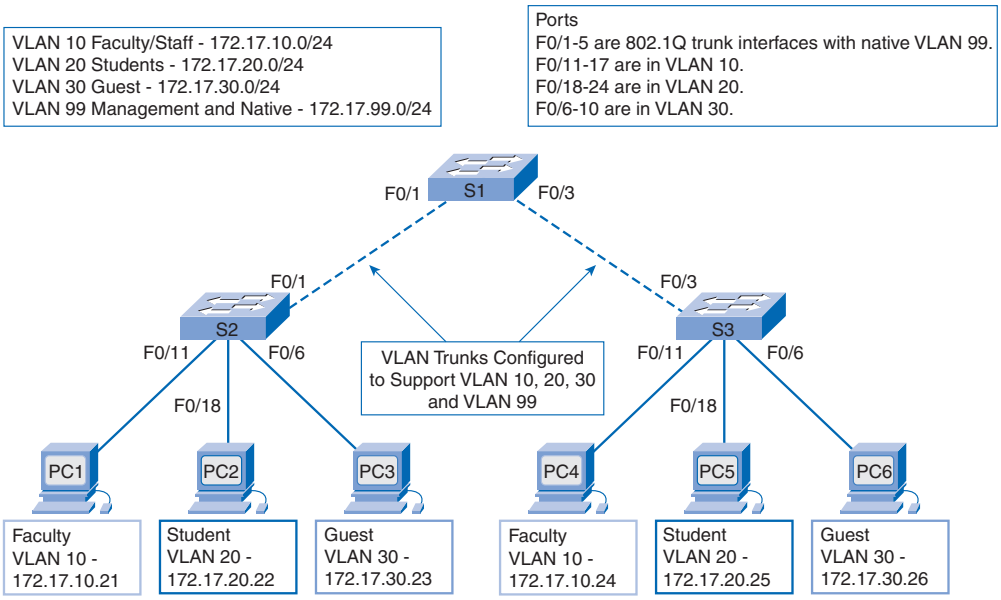
Investigating a VLAN Implementation (3.1.4)

Use the Packet Tracer Activity to observe how broadcast traffic is forwarded by the switches when VLANs are configured and when VLANs are not configured. Use File e3-3144.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

VLAN Trunking

VLANs and VLAN trunks are inextricably linked. VLANs in a modern switched LAN would be practically useless without VLAN trunks. We know that VLANs control network broadcasts, and we know that VLAN trunks transmit traffic to different parts of the network within a given VLAN. In Figure 3-22, the links between switches S1 and S2, and S1 and S3, are configured to transmit traffic coming from VLAN 10, 20, 30, and 99. This network simply could not function without VLAN trunks. You will find that most networks that you encounter are configured with VLAN trunks. This section brings together the knowledge you already have on VLAN trunking and delves into the details necessary for a complete conceptual understanding of the role of trunks in a switched LAN.

Figure 3-22 VLAN Trunking



VLAN Trunks

A ***VLAN trunk*** is an Ethernet point-to-point link between an Ethernet switch interface and an Ethernet interface on another networking device, such as a router or a switch, carrying the traffic of multiple VLANs over the singular link. A VLAN trunk allows you to extend the VLANs across an entire network. Cisco switches support IEEE 802.1Q for trunk formation on Fast Ethernet and Gigabit Ethernet interfaces. You learn about 802.1Q later in this section. A VLAN trunk does not belong to a specific VLAN, but rather it serves as a conduit for VLANs between switches.

In Figure 3-23, you see the standard topology used in this chapter, except that instead of the VLAN trunk you are used to seeing between switches S1 and S2, a separate link exists for each subnet. Four separate links connect switches S1 and S2, leaving three fewer ports to allocate to end-user devices. Each time a new subnetwork is needed, a new link is required for each switch in the network.

In Figure 3-24, the network topology shows a VLAN trunk connecting switches S1 and S2 with a single physical link. This is the way a network should be configured. The four separate links in Figure 3-23 have been replaced by a single trunk link.

Figure 3-23 Without VLAN Trunks

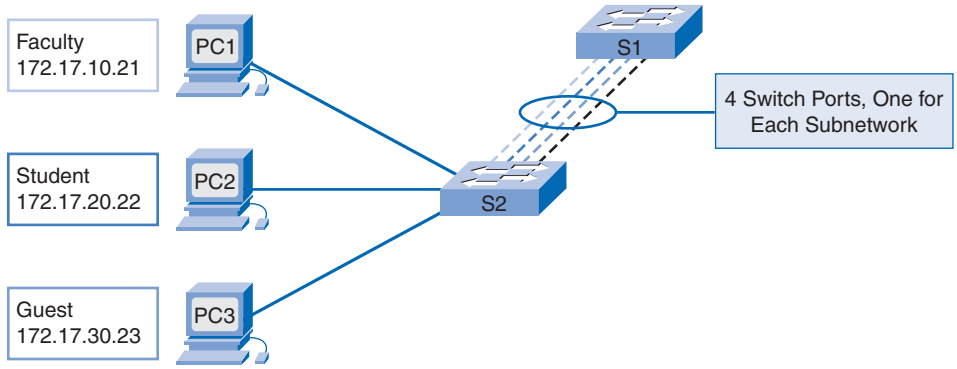
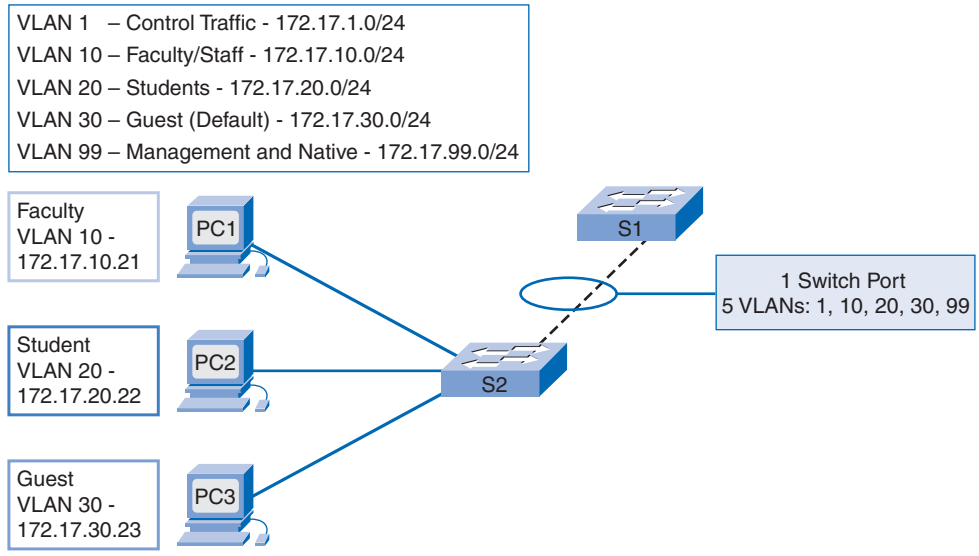


Figure 3-24 With VLAN Trunks



IEEE 802.1Q Frame Tagging

Access layer switches are Layer 2 devices. They use only the Ethernet frame header information to forward frames. When an Ethernet frame arrives on an access port from a connected device, the frame header does not contain information about which VLAN the frame belongs to. Subsequently, when Ethernet frames are placed on a trunk, they need additional information about the VLANs they belong to. This is accomplished by using 802.1Q frame tagging. This header adds a tag to the original Ethernet frame specifying the VLAN to which the frame belongs.

We briefly discussed frame tagging earlier in the context of voice-enabled switch ports, where voice frames are tagged to differentiate them from data frames destined for the computer attached to the IP phone, which is directly connected to the access port. You also learned that VLAN IDs can be in a normal range, 1–1005, or an extended range, 1006–4094. But how do VLAN IDs get inserted into an Ethernet frame?

Before exploring the details of 802.1Q tag fields, it is helpful to understand what a switch does when it forwards a frame out a trunk link. Roughly, when a switch receives a frame on a port configured in access mode (static VLAN) and destined for a remote device via a trunk link, the switch takes apart the frame and inserts a VLAN tag, recalculates the FCS, and sends the tagged frame out the trunk port.

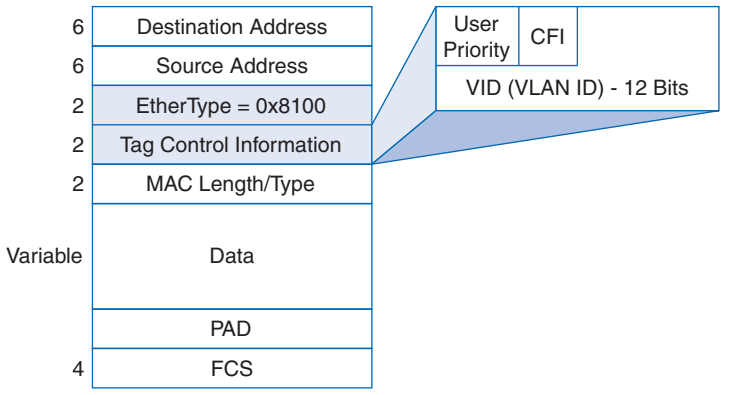
The VLAN tag field consists of an EtherType field and a tag control information field.

The EtherType field is set to the hexadecimal value of 0x8100. This value is called the tag protocol ID (TPID) value. With the EtherType field set to the TPID value, the switch receiving the frame knows to look for information in the tag control information field.

The tag control information field, shown in Figure 3-25, contains the following:

- **3 bits of user priority:** Used by the ***IEEE 802.1p*** standard, which specifies how to provide expedited transmission of Layer 2 frames. A description of the IEEE 802.1p is beyond the scope of this book; however, you learned a little about it earlier in the discussion on voice VLANs.
- **1 bit of *Canonical Format Identifier (CFI)*:** Enables Token Ring frames to be carried across Ethernet links easily.
- **12 bits of *VLAN ID (VID)*:** VLAN identification numbers; supports up to 4096 VLAN IDs.

Figure 3-25 IEEE 802.1Q VLAN Tag Fields



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

Native VLANs

Now that you know more about how a switch tags a frame with the appropriate VLAN, it is time to explore how the native VLAN supports the switch in handling tagged and ***untagged frames*** that arrive or are sent on an 802.1Q trunk port.

Some devices that support trunking tag native VLAN traffic as a default behavior. If an 802.1Q trunk port receives a tagged frame on the native VLAN, it drops the frame. Consequently, when configuring a switch port on a Cisco Catalyst switch, you need to identify these devices and configure them 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.

When a Cisco switch trunk port receives untagged frames, it forwards those frames to the native VLAN. As you may recall, the default native VLAN is VLAN 1. When you configure an 802.1Q trunk port, a Port VLAN ID (PVID) is assigned to the port according to the value of the native VLAN ID. All untagged traffic coming in 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 Table 3-1, VLAN 99 is configured as the native VLAN on port F0/1 of switch S1, changing it from the default value of 1.

Table 3-1 Native VLAN Trunk Configuration

Description	CLI
Enter global configuration mode on switch S1.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface f0/1`
Configure the VLAN 99 to send and receive untagged traffic on the trunk port F0/1. The range for vlan-id is 1 to 4094.	`S1(config-if)# switchport trunk native vlan 99`
Return to privileged EXEC mode.	`S1(config-if)# end`

Using the **show interfaces** *interface-id* **switchport** command, you can quickly verify that you have correctly reconfigured the native VLAN from VLAN 1 to VLAN 99. In Example 3-4, the highlighted output indicates that the configuration was successful.

Example 3-4 Voice VLAN Configuration

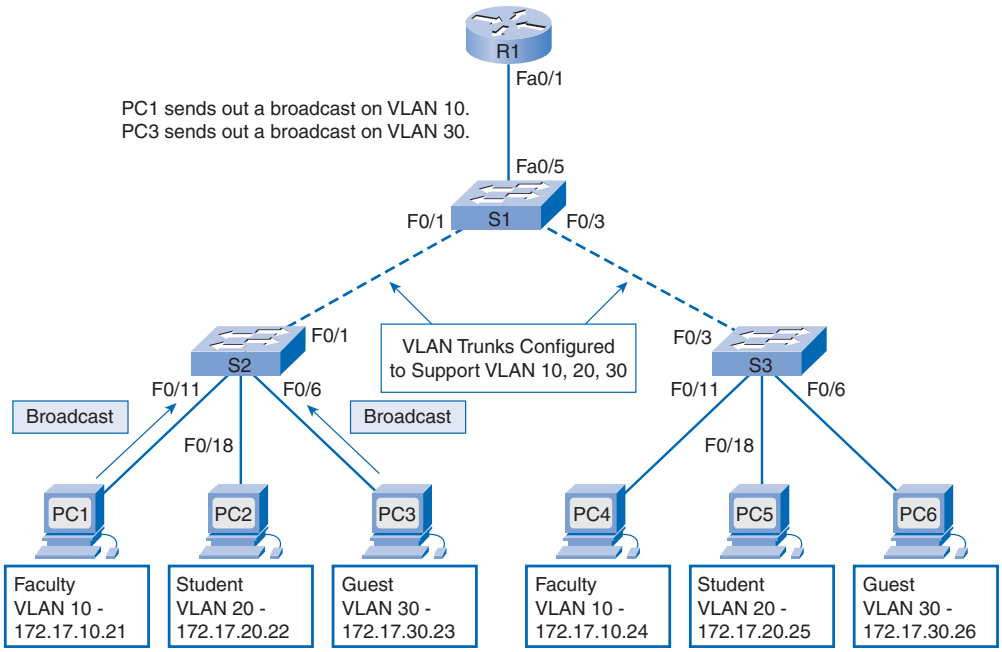
```
S1# show interfaces F0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
```

```
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 50
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
<output omitted>
Trunking VLANs Enabled: ALL
```

Trunking Operation

You have learned how a switch handles untagged traffic on a trunk link: Frames traversing a trunk link are tagged with the VLAN ID of the access port the frame arrived on, or they remain untagged if associated with the native VLAN. In Figure 3-26, PC1 on VLAN 10 and PC3 on VLAN 30 send broadcast frames to switch S2. Switch S2 tags these frames with the appropriate VLAN ID and then forwards the frames over the trunk to switch S1. Switch S1 reads the VLAN ID on the frames and broadcasts them to each port configured to support VLAN 10 and VLAN 30, respectively. Switch S3 receives these frames, strips off the VLAN IDs, and forwards the untagged frames to PC4 on VLAN 10 and PC6 on VLAN 30.

Figure 3-26 Trunking Operation



Trunking Modes

You have learned how 802.1Q trunking works on Cisco Catalyst switch ports. Now it is time to examine the 802.1Q trunk port mode configuration options. First we need to discuss a Cisco legacy trunking protocol called ***inter-switch link (ISL)***, because you will see this option in the switch software configuration guides, and it is supported by all current Cisco Catalyst switches other than the Catalyst 29xx series switches.

Although most Cisco Catalyst switches can be configured to support two types of trunk ports, IEEE 802.1Q and ISL, today only 802.1Q is used in practice. However, legacy networks may still use ISL, and it is useful to be aware of each trunk encapsulation option:

- An IEEE 802.1Q trunk port simultaneously supports both tagged and untagged traffic. An 802.1Q trunk port is assigned a default PVID, which is associated with all untagged traffic on the port. All traffic with a null VLAN ID is assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.
- With ISL trunk ports, all received packets are expected to be encapsulated with an ISL header, and all transmitted packets are sent with an ISL header. Native (nontagged) frames received from an ISL trunk port are dropped. ISL is no longer a recommended trunk port mode, and it is not supported on a number of Cisco Catalyst switches.

Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol that negotiates both the status of trunk ports as well as the trunk encapsulation of trunk ports. Switches from other vendors do not support DTP. DTP is automatically enabled on a switch port when certain ***trunking modes*** are configured on the switch port. DTP manages trunk negotiation only if the port on the other switch is configured in a trunk mode that supports DTP. DTP supports both ISL and 802.1Q trunks. This book focuses on the 802.1Q implementation of DTP; a detailed discussion on DTP is beyond the scope of this book. Switches do not need DTP to enable trunks, and some Cisco switches and routers do not support DTP.

A switch port on a Cisco Catalyst switch supports a number of trunking modes. The trunking mode defines how the port negotiates using DTP to set up a trunk link with its peer port. The following provides a brief description of the available trunking modes and how DTP is implemented in each.

- The switch port periodically sends DTP frames, called advertisements, to the remote port. The command used is **switchport mode trunk** and is the default configuration. The local switch port advertises to the remote port that it is dynamically changing to a trunking state. The local port then, regardless of what DTP information the remote port sends as a response to the advertisement, changes to a trunking state. The local port is considered to be in an unconditional (always on) trunking state.
- The switch port periodically sends DTP frames to the remote port. The command used is **switchport mode dynamic auto**. The local switch port advertises to the remote switch port that it is able to trunk but does not request to go to the trunking state. After

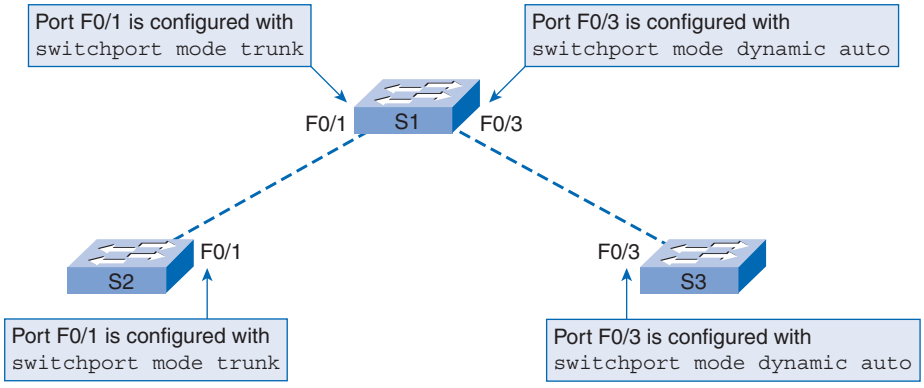
a DTP negotiation, the local port ends up in trunking state only if the remote port trunk mode has been configured to be **on** or **desirable**. If both ports on the switches are set to **auto**, they do not negotiate to be in a trunking state. They negotiate to be in the access (nontrunk) mode state.

- DTP frames are sent periodically to the remote port. The command used is **switchport mode dynamic desirable**. The local switch port advertises to the remote switch port that it is able to trunk and asks the remote switch port to go to the trunking state. If the local port detects that the remote has been configured in **on**, **desirable**, or **auto** mode, the local port ends up in trunking state. If the remote switch port is in the ***nonegotiate*** mode, the local switch port remains as a nontrunking port.
- You can turn off DTP for the trunk so that the local port does not send out DTP frames to the remote port. Use the command **switchport nonegotiate**. The local port is then considered to be in an unconditional trunking state. Use this feature when you need to configure a trunk with a switch from another switch vendor.

To learn about DTP support on Cisco switches, visit www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml.

As an example, refer to Figure 3-27 with three Catalyst 2960 switches represented. The F0/1 ports on switches S1 and S2 are configured with trunk mode **on** (**switchport mode trunk**). The F0/3 ports on switches S1 and S3 are configured as ***dynamic auto*** (**switchport mode dynamic auto**). When the switch configurations are complete and the switches are fully configured, which links will be active trunks?

Figure 3-27 Dynamic Trunking Protocol



The link between switches S1 and S2 becomes an active trunk because the F0/1 ports on switches S1 and S2 are configured to ignore all DTP advertisements. The F0/3 ports on switches S1 and S3 are set to **auto**; in this case, the result is an inactive trunk link because the ports negotiate to be in the access (nontrunk) mode state.

Note

The default switchport mode for an interface on a Catalyst 2950 switch is ***dynamic desirable***, but the default switchport mode for an interface on a Catalyst 2960 switch is dynamic auto. If S1 and S3 were Catalyst 2950 switches with interface F0/3 in default switchport mode, the link between S1 and S3 would become an active trunk.

As a very useful reference giving the results of trunk status based on the various DTP configuration options on Catalyst 2960 switches, see Table 3-2.

Table 3-2 Trunk Negotiation Combinations

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not Recommended
Access	Access	Access	Not Recommended	Access

Use the **show dtp interface** privileged EXEC command, introduced in IOS Release 12.2(37)EY on Catalyst 2960 switches, to determine the current settings.

For information on which Cisco switches support 802.1Q, ISL, and DTP, visit www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml#topic1.

For information on how to support ISL on legacy networks, visit www.cisco.com/en/US/tech/tk389/tk689/tsd_technology_support_troubleshooting_technotes_list.html.

Packet Tracer Activity

Investigating VLAN Trunks (3.2.3)

Use this Packet Tracer Activity to practice working with VLAN trunks. Trunks carry the traffic of multiple VLANs through a single link, making them a vital part of communicating between switches with VLANs. This activity focuses on viewing switch configuration, trunk configuration, and VLAN tagging information. Use file e3-3232.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Configure VLANs and Trunks

In this chapter, you have already seen some examples of the commands used to configure VLANs and VLAN trunks. In this section, you learn the key Cisco IOS commands needed to create, delete, and verify VLANs and VLAN trunks. Often these commands have many optional parameters that extend the capabilities of the VLAN and VLAN trunk technology.

Some specialized optional commands are not presented; however, references are provided if you want to research these options. The focus of this section is to provide you with the ability to confidently configure VLANs and VLAN trunks with their key features.

Configure a VLAN

In this section we discuss the configuration of static VLANs on Cisco Catalyst switches. Two different modes exist for configuring VLANs on a Cisco Catalyst switch: database configuration mode and global configuration mode. Although the Cisco documentation mentions VLAN database configuration mode, it is being deprecated in favor of VLAN global configuration mode. It is evident that the database configuration mode will eventually go away; the intent of the change is to migrate the switch operating system toward a more Cisco-routerlike operating system. Over the years, the line between Cisco routers and Catalyst switches is becoming increasingly blurred.

You will configure VLANs with IDs in the normal range. Recall that there are two ranges of VLAN IDs. The normal range includes IDs 1 to 1001, and extended range consists of IDs 1006 to 4094. VLAN 1 and 1002 to 1005 are reserved ID numbers. When you configure normal range VLANs, the configuration details are stored automatically in Flash memory on the switch in a file called vlan.dat. Because you often configure other aspects of a Catalyst switch at the same time, it is good practice to save running-config file changes to the startup-config file.

Table 3-3 reviews the Cisco IOS commands used to add a VLAN to a switch.

Table 3-3 Adding a VLAN

Description	CLI
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN. vlan-id is the VLAN number that is to be created. The CLI switches to VLAN configuration mode for VLAN vlan-id.	`S1(config)# vlan vlan-id`
(Optional) Specify a unique VLAN name to identify the VLAN. If no name is entered, the VLAN number, with padded zeros, is appended to the word "VLAN"; for example, VLAN0020.	`S1(config-vlan)# name vlan-name`
Return to privileged EXEC mode. You must end your configuration session for the configuration to be saved in the vlan.dat file and for configuration to take effect.	`S1(config-vlan)# end`

Figure 3-28 shows a basic topology with the student VLAN, VLAN 20, being configured on switch S1.

Figure 3-28 Switch Topology for Basic VLAN Configuration

Example 3-5 displays commands for adding VLAN 20.

Example 3-5 Adding a VLAN

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

Example 3-6 demonstrates the use of the **show vlan brief** command to display the contents of the vlan.dat file. The student VLAN, VLAN 20, is highlighted. The default VLAN IDs of 1 and 1002 to 1005 can be seen in the output. Notice that no ports are configured yet for VLAN 20.

Example 3-6 show vlan brief

```
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, Fa0/11, 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
```

Interface F0/18 is connected to the student computer, PC2, and must be added to VLAN 20. Example 3-7 demonstrates the configuration commands. A static access port can belong to only one VLAN at a time. When VLAN 20 is configured on other switches, the switch administrator configures the other student computers to be in the same subnet as PC2: 172.17.20.0/24.

Example 3-7 Static VLAN Interface Configuration

```
S1# configure terminal
S1(config)# interface f0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
```

After adding interface F0/18 to VLAN 20, the **show vlan brief** output changes, as seen in Example 3-8.

Example 3-8 show vlan brief Updated

```
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, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
20   student                           active    Fa0/18
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Note

In addition to entering a single VLAN ID, you can enter a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens using the **vlan** *vlan-id* command; for example: switch(config)# **vlan 100,102,105-107**.

Managing VLANs

After you configure a VLAN, you can validate the VLAN configurations using Cisco IOS show commands. The command syntax for the **show vlan** command is

```
show vlan [brief ¦ id vlan-id ¦ name vlan-name ¦ summary]
```

The syntax is explained in Table 3-4.

Table 3-4 **show vlan** Command Syntax

Explanation	Syntax
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**

The command syntax for the **show interfaces switchport** command is the following:

```
show interfaces [interface-id ¦ vlan vlan-id] ¦ switchport
```

The syntax is explained in Table 3-5.

Table 3-5 **show interfaces switchport** Command Syntax

Explanation	Syntax
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 4094.	**vlan** *vlan-id*
Display the administrative and operational status of a switching port, including port blocking and port protection settings.	**switchport**

In Example 3-9, you can see that the **show vlan name student** command does not produce clearly discernible output. The preference here is to use the **show vlan brief** command, as in Example 3-8.

Example 3-9 show vlan name Output

```
S1# show vlan name student

VLAN Name                              Status    Ports
---------------------------------------------------------------------------
20   student                           active    Fa0/18

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
---------------------------------------------------------------------------
```

The **show vlan summary** command output, shown in Example 3-10, displays the count of all configured VLANs. The output shows six VLANs: 1, 1002–1005, and the student VLAN, VLAN 20.

Example 3-10 show vlan summary Output

```
S1# show vlan summary
Number of existing VLANs              : 6
Number of existing VTP VLANs          : 6
Number of existing extended VLANs     : 0
```

The **show interfaces vlan 20** command displays detail that is beyond the scope of this chapter. The key information appears on the second line of the output in Example 3-11, indicating that VLAN 20 is up.

Example 3-11 show interfaces Output

```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia 001c.573c.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 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 multicast)
   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
```

The **show interfaces switchport** command is one of the most useful commands on a Catalyst switch. It displays pertinent information about the referenced interface(s). In Example 3-12, you can see that the F0/18 is assigned to VLAN 20 and that the native VLAN is VLAN 1. We used this command once before in the context of voice VLANs.

Example 3-12 show interfaces switchport Output

```
S1# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association:10 (VLAN0010) 502 (VLAN0502)
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 private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

```
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

For more details on the **show vlan** and **show interfaces** command output fields, visit www.cisco.com/en/US/products/ps6406/products_command_reference_chapter09186a008081874b.html#wp7730585.

Managing VLAN Memberships

You can manage VLANs and VLAN port memberships in a number of ways. Table 3-6 explains the commands for removing VLAN membership.

Table 3-6 Managing VLAN Membership

Description	CLI
Enter global configuration mode.	`S1# configure terminal`
Enter the interface configuration mode for the interface to be configured.	`S1(config)# interface interface-id`
Remove the VLAN assignment on that switch port interface and revert to the default VLAN membership of VLAN 1.	`S1(config-if)# no switchport access vlan`
Return to privileged EXEC mode.	`S1(config-if)# end`

To reassign a port to VLAN 1, you can use the **no switchport access vlan** command in interface configuration mode. After entering this command, examine the output of the **show vlan brief** command in Example 3-13. Notice how VLAN 20 is still active. Interface F0/18 has been removed from VLAN 20. The **show interfaces f0/18 switchport** command shows that the access VLAN for interface F0/18 has been reset to VLAN 1.

Example 3-13 Reassign Port to VLAN 1

```
S1(config)# interface f0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
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, Fa0/11, 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
S1# show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
<output omitted>
```

A static access port can have only one VLAN. With Cisco IOS software, you do not need to first remove a port from a VLAN to change its VLAN membership. When you reassign a static access port to an existing VLAN, the port is automatically removed from the previous VLAN. In Example 3-14, port F0/11 has been reassigned to VLAN 20.

Example 3-14 Reassign Port to VLAN 20

```
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
```

Example 3-15 demonstrates the deletion of a VLAN with the global configuration command **no vlan** *vlan-id*. The **show vlan brief** command verifies that VLAN 20 is no longer in the vlan.dat file.

Example 3-15 Deleting a VLAN

```
S1# no vlan 20
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
```

Alternatively, the entire vlan.dat file can be deleted using the command **delete flash:vlan.dat** in privileged EXEC mode. After the switch is reloaded, the previously configured VLANs will no longer be present. This effectively places the switch into "factory default" condition with its VLAN configuration.

Note

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 remain members of the deleted inactive VLAN and are unable to communicate with other systems after you delete the VLAN.

Configure a Trunk

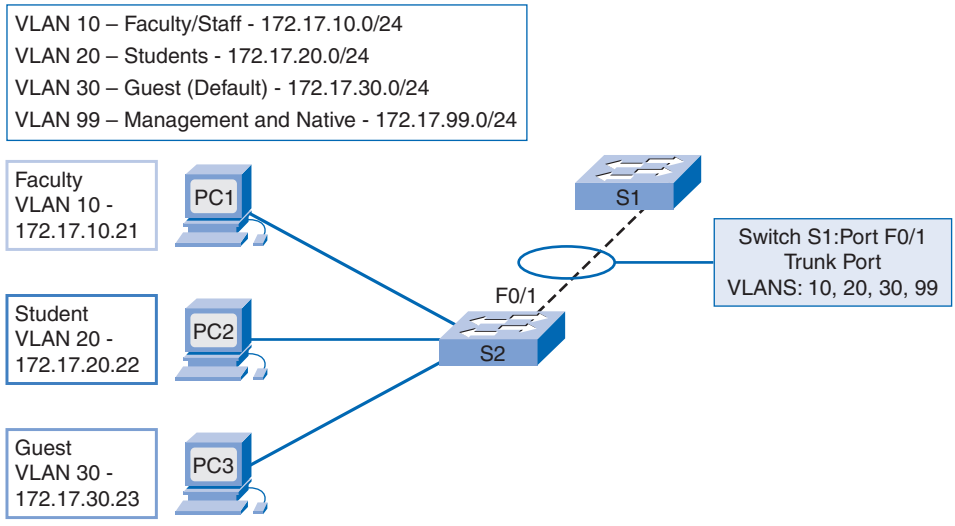
To configure a trunk on a switch port, use the **switchport mode trunk** command. When you enter this command on a switch port, the interface changes to permanent trunking mode, and the port enters into a DTP negotiation to convert the link into a trunk, even if the opposing interface does not agree to the change. In this book, you configure a trunk using the **switchport mode trunk** command. The Cisco IOS command syntax to specify a native VLAN other than VLAN 1 is also shown in Table 3-7.

Table 3-7 IEEE 802.1Q Trunk Configuration

Description	CLI
Enter global configuration mode.	`S1# configure terminal`
Enter the interface configuration mode for the defined interface.	`S1(config)# interface interface-id`
Force the link connecting the switches to be a trunk link.	`S1(config-if)# switchport mode trunk`
Specify another VLAN as the native VLAN for untagged frames for IEEE 802.1Q trunks.	`S1(config-if)# switchport trunk native vlan vlan-id`
Add the VLANs allowed on this trunk.	`S1(config-if)# switchport trunk allowed vlan add vlan-list`
Return to privileged EXEC mode.	`S1(config-if)# end`

Refer to Figure 3-29. VLANs 10, 20, and 30 support the Faculty, Student, and Guest computers: PC1, PC2, and PC3. The F0/1 port on switch S1 will be configured as a trunk port to allow only VLANs 1, 10, 20, and 30 (recall that VLAN 1 is unconditionally supported on a trunk link, as all control traffic is associated with VLAN 1). VLAN 99 will be configured as the native VLAN.

Figure 3-29 Enabling a Trunk Link



Example 3-16 demonstrates the configuration of switch S1. Port F0/1 is configured as the trunk port. The native VLAN is reconfigured from VLAN 1 to VLAN 99, with VLANs 10, 20, and 30 on port F0/1.

Example 3-16 Enabling a Restricted Trunk Link

```
S1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan add 10,20,30
S1(config-if)# end
```

For more detail on all the parameters associated with the **switchport mode** interface command, visit www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_37_se/command/reference/cli3.html#wp1948171.

Example 3-17 displays the administrative and operational status of switch port F0/1 on switch S1. The command used is the **show interfaces** *interface-ID* **switchport** command.

Example 3-17 Verify Trunk Configuration

```
S1#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
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 private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
<output omitted>
```

The first highlighted area shows that port F0/1 has its administrative mode set to trunk; the port is set to form a trunk regardless of the configuration of the opposing interface. The

next highlighted area verifies that the native VLAN is VLAN 99. The last highlighted area shows that the enabled trunking VLANs are VLANs 10, 20, and 30.

Table 3-8 displays the commands to reset the ***allowed VLANs*** and the native VLAN of the trunk to the default state. The command to reset the switch port to an access port and remove the trunk is also shown.

Table 3-8 IEEE 802.1Q Trunk Modification

Description	CLI
Use this command in the interface configuration mode to reset all the VLANs configured on the trunk interface.	`S1(config-if)# no switchport trunk allowed vlan`
Use this command in the interface configuration mode to reset the native VLAN back to VLAN 1.	`S1(config-if)# no switchport trunk native vlan`
Use this command in the interface configuration mode to reset the trunk port back to a static access mode port.	`S1(config-if)# switchport mode access`

Example 3-18 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 3-18 Resetting a Trunk

```
S1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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: 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>
Trunking VLANs Enabled: ALL
```

Last, in Example 3-19, the output demonstrates the commands used to remove the trunk from the F0/1 switch port on switch S1. The **show interfaces f0/1 switchport** command reveals that the F0/1 interface is in static access mode.

Example 3-19 Removing a Trunk

```
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
Operatioss Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
<output omitted>
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Packet Tracer Activity

Configuring VLANs and Trunks (3.3.4)

Use this Packet Tracer Activity to enhance your skills with VLAN and VLAN trunk configuration. 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, assigning access ports to specific VLANs, changing the native VLAN, and configuring trunk links. Use File e3-3344.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Troubleshooting VLANs and Trunks

Common VLAN and trunking issues are usually associated with incorrect configurations. When you configure VLANs and trunks on a switched infrastructure, these configuration errors occur in decreasing frequency as follows:

- **Native VLAN mismatches:** Trunk ports are configured with different native VLANs—for example, if one port has defined VLAN 99 as the native VLAN and the other trunk port has defined VLAN 100 as the native VLAN. This configuration error generates console notifications, causes control and management traffic to be misdirected, and poses a security risk.

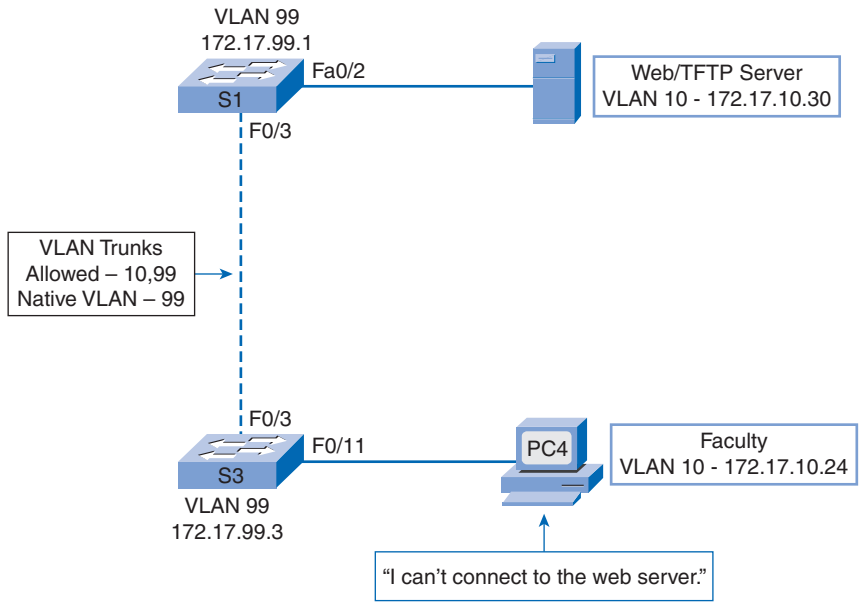
- **Trunk mode mismatches:** One trunk port is configured with trunk mode "off" and the other with trunk mode "on". This configuration error causes the trunk link to stop working.
- **VLANs and IP subnets:** User computers, for example, may have been configured with the incorrect IP addresses or subnet masks or default gateways. The result is loss of connectivity.
- **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.

If you have discovered an issue with a VLAN or trunk and do not know what the problem is, start your troubleshooting by examining the trunks for a native VLAN mismatch and then work down the list. The rest of this topic examines how to fix the common problems with trunks.

Common Problems with Trunks

Refer to Figure 3-30. You are a network administrator and you get a call that the person using computer PC4 cannot connect to the internal web server, the web/TFTP Server. You learn that a new technician was recently configuring switch S3. The topology diagram seems correct, so why does a problem exist? You decide to check the configuration on S3.

Figure 3-30 Native VLAN Issues



As soon as you connect to switch S3, the error message shown in the top highlighted area in Example 3-20 appears in your console window. You take a look at the interface using the **show interfaces f0/3 switchport** command. You notice that the native VLAN, the second highlighted area in the example, has been set to VLAN 100 and is inactive. As you scan further down the output, you see that the allowed VLANs are 10 and 99, shown in the bottom highlighted area.

Example 3-20 Native VLAN Mismatch

```
S3#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3
  (100), with S1 FastEthernet0/1 (99).
S3# show interfaces f0/3 switchport
Name: Fa0/3
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: 100 (Inactive)
<output omitted>
Trunking VLANs Enabled: 10,99
<output omitted>
```

You need to reconfigure the native VLAN on trunk port F0/3 to VLAN 99. In Example 3-21, the top highlighted area shows the command to configure the native VLAN as VLAN 99. The next two highlighted areas confirm that the trunk port F0/3 has the native VLAN reset to VLAN 99.

Example 3-21 Native VLAN Fix

```
S3# configure terminal
S3(config)# interface f0/3
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# end
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
<output omitted>
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
<output omitted>
Trunking VLANs Enabled: 10,99
<output omitted>
```

The screen output in Example 3-22 for the computer PC4 shows that connectivity has been restored to the Web/TFTP server found at IP address 172.17.10.30.

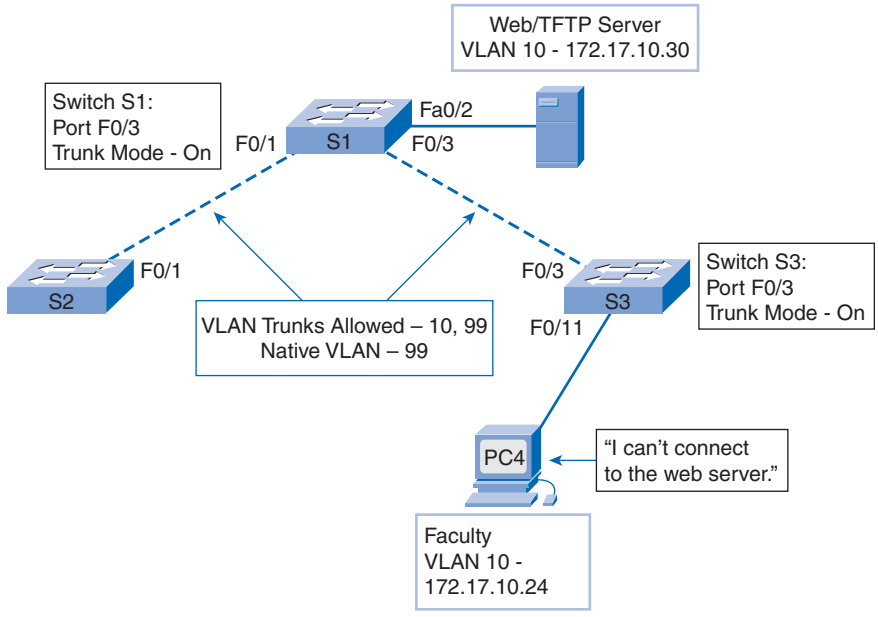
Example 3-22 Connectivity Test

```
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>
```

You have configured trunks manually with the **switchport mode trunk** command. You also learned that the trunk ports use DTP advertisements to negotiate the state of the link with the remote port. When a port on a trunk link is configured with a trunk mode that is incompatible with the other trunk port, a trunk link fails to form between the two switches.

For the next trunk troubleshooting scenario, refer to Figure 3-31.

Figure 3-31 Trunk Mode Issues



In this scenario, the person using computer PC4 cannot connect to the internal web server. Figure 3-31 show a topology diagram with the current configuration settings. What is the problem?

The first thing you do is check the status of the trunk ports on switch S1 using the **show interfaces trunk** command, as shown in Example 3-23. It reveals that there is not a trunk

on interface F0/3 on switch S1. You examine interface F0/3 to learn that the switch port is in dynamic auto mode, the first highlighted area in the top figure. An examination of the trunks on switch S3 reveals that are no active trunk ports. Further checking reveals that the F0/3 interface is also in dynamic auto mode, as seen in the first highlighted area in the bottom of Example 3-23. The trunk is down because both ends are in dynamic auto mode.

Example 3-23 show interfaces trunk and show interfaces switchport

```
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 interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto

S3# show interfaces trunk

S3#
S3# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
<output omitted>
```

You need to reconfigure the trunk mode of the F0/3 ports on switches S1 and S3 (or at least one of the ports). In the top of Example 3-24, the highlighted area shows that the switch S1 F0/3 port is now in trunking mode. The output for switch S3 shows the commands used to reconfigure the port as well as the results of the **show interfaces switchport** and **show interfaces trunk** command, revealing that interface F0/3 has been reconfigured as a trunk. The output from computer PC4 indicates that PC4 has regained connectivity to the web/TFTP server found at IP address 172.17.10.30.

Example 3-24 show interfaces trunk

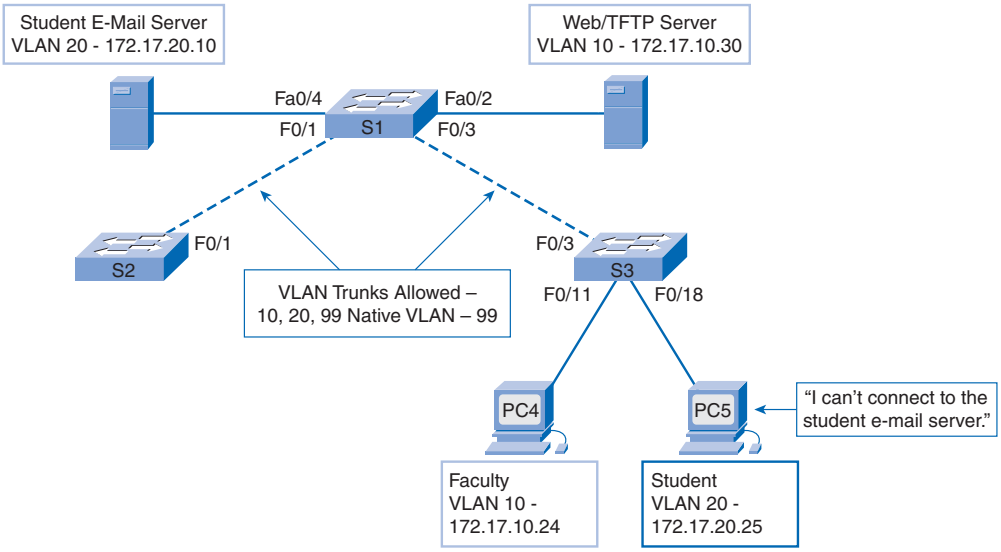
```
S1# configure terminal
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
```

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

S3# configure terminal
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
S3#

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>
```

For the final trunk troubleshooting scenario, refer to Figure 3-32. You have learned that for traffic from a VLAN to be transmitted across a trunk, it has to be allowed on the trunk. The command used to do this is the **switchport trunk allowed vlan** *vlan-list* command. In Figure 3-32, VLAN 20 (Student) and computer 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, the person using computer PC5 cannot connect to the student e-mail server shown in Figure 3-32.

Figure 3-32 Allowed VLAN List Issues



You check the trunk ports on switch S1 using the **show interfaces trunk** command, as illustrated in Example 3-25. The command reveals that interface F0/3 on switch S3 is correctly configured to allow VLANs 10, 20, and 99. An examination of interface F0/3 on switch S1 reveals that interfaces F0/1 and F0/3 allow only VLANs 10 and 99. It seems someone updated the documentation but forgot to reconfigure the ports on the S1 switch.

Example 3-25 Allowed VLANs in **show interfaces trunk**

```
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>
S1#
```

You need to reconfigure the F0/1 and the F0/3 ports on switch S1 using the **switchport trunk allowed vlan 10,20,99** command. Example 3-26 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. Last, Example 3-26 shows that PC5 has regained connectivity to the student e-mail server at 172.17.20.10.

Example 3-26 switchport trunk allowed vlan *vlan-list*

```
S1# configure terminal
S1(config)# 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

PC5> ping 172.17.20.10
Pinging 172.17.20.10 with 32 bytes of data:
Reply from 172.17.20.10: bytes=32 time=147ms TTL=128
<output omitted>
```

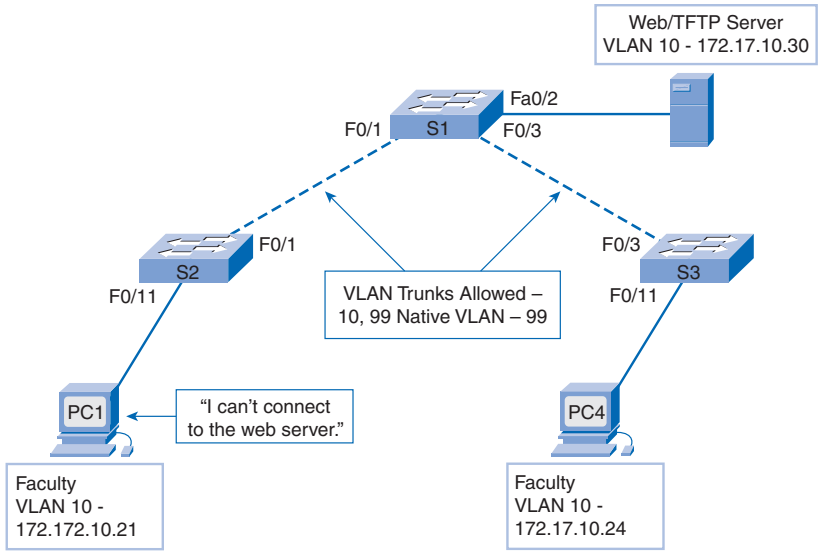
A Common Problem with VLAN Configurations

In modern switched LANs, each VLAN corresponds to a unique IP subnet. If two devices in the same VLAN have different subnet IP addresses, they cannot communicate. This type of incorrect configuration is not uncommon, and it is easy to solve by identifying the offending device and changing the subnet IP addresses to the correct ones.

In the scenario pictured in Figure 3-33, the person using PC1 cannot connect to the faculty web server.

In Example 3-27, a check of the IP configuration settings of PC1 reveals the most common error in configuring VLANs: an incorrectly configured IP address. The PC1 computer is configured with an IP address of 172.172.10.21, but it should have been configured with 172.17.10.21; the mistake results in PC1 being on the wrong subnet.

Figure 3-33 VLAN Configuration Issues



Example 3-27 IP Addressing on LAN Workstation

```
PC1> ipconfig

IP Address.....................: 172.172.10.21
Subnet Mask....................: 255.255.255.0
Default Gateway................: 0.0.0.0

PC1>
```

After changing the IP address of PC1 to 172.17.10.21, Example 3-28 reveals that PC1 has regained connectivity to the web/TFTP server found at IP address 172.17.10.30.

Example 3-28 Connectivity Test After IP Address Adjustment

```
PC1> 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>
```

Packet Tracer Activity

Troubleshooting a VLAN Implementation (3.4.2)

Use this Packet Tracer Activity to troubleshoot connectivity problems between PCs on the same VLAN. Use File e3-3422.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Summary

In this chapter, we introduced VLANs. VLANs are used to segment broadcast domains in a switched LAN. This improves the performance and manageability of LANs. VLANs provide network administrators flexible control over traffic associated with devices in the LAN.

The principal type of VLANs are data VLANs, the default VLAN, the black hole VLAN, native VLANs, management VLANs, and voice VLANs.

VLAN trunks facilitate interswitch communication with multiple VLANs. IEEE 802.1Q frame tagging enables differentiation between Ethernet frames associated with distinct VLANs as they traverse common trunk links.

We discussed the configuration, verification, and troubleshooting of VLANs and VLAN trunks using the Cisco IOS CLI.

Labs

The labs available in the companion *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-202-8) provide hands-on practice with the following topics introduced in this chapter:

Lab 3-1: Basic VLAN Configuration (3.5.1)

In this lab, you are guided to limit the effects of network broadcasts. One way to do this is to break up a large physical network into a number of smaller logical or virtual networks. This is one of the goals of VLANs. This lab teaches you the basics of configuring VLANs.

Lab 3-2: Challenge VLAN Configuration (3.5.2)

In this lab, with minimal guidance you limit the effects of network broadcasts. One way to do this is to break up a large physical network into a number of smaller logical or virtual networks. This is one of the goals of VLANs. This lab teaches you the basics of configuring VLANs.

Lab 3-3: Troubleshooting VLAN Configurations (3.5.3)

In this lab, you troubleshoot a misconfigured VLAN environment. You or your instructor loads the provided configurations into your lab equipment. Your objective is to locate and correct any and all errors in the configurations and establish end-to-end connectivity. Your final configuration should match the provided topology diagram and addressing table.

Many of the hands-on labs include Packet Tracer Companion Activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-202-8) for hands-on labs that have a Packet Tracer Companion.

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. Answers are listed in the Appendix, "Check Your Understanding and Challenge Questions Answer Key."

1. Switch S1 and Switch S2 are both configured with ports in the Marketing, Sales, Production, and Admin VLANs. Each VLAN contains 12 users. How many subnets are needed to address the VLANs?

   A. 1
   B. 2
   C. 4
   D. 8
   E. 12
   F. 24

2. What mechanism is used to achieve the separation between different VLANs as they cross a trunk link?

   A. VLAN tagging using 802.1Q protocol
   B. VLAN tagging using 802.1p protocol
   C. VLAN multiplexing
   D. VLAN set as a native VLAN

3. What are two options to consider when configuring a trunk link between two switches? (Choose two.)

   A. The **switchport nonegotiate** command must be configured for trunks that use DTP.
   B. Port security cannot be configured on the trunk interfaces.
   C. The native VLAN must be the same on both ends of the trunk.
   D. Different encapsulation types can be configured on both ends of the trunk link.
   E. Trunk ports can be configured only on Gigabit Ethernet interfaces.

4. A 12-port switch has been configured to support three VLANs named Sales, Marketing, and Finance. Each VLAN spans four ports on the switch. The network administrator has deleted the Marketing VLAN from the switch. What two statements describe the status of the ports associated with this VLAN? (Choose two.)

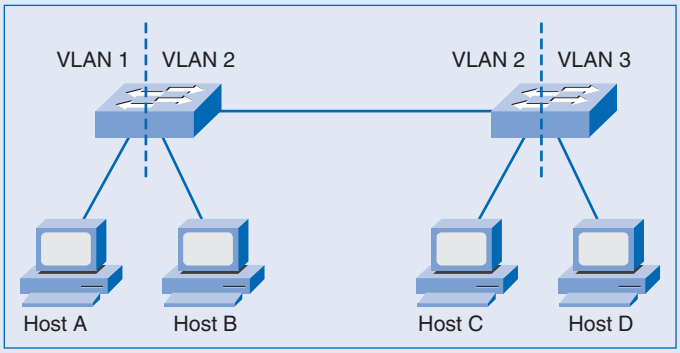
   A. The ports are inactive.
   B. The ports are administratively disabled.
   C. The ports will become trunks to carry data from all remaining VLANs.
   D. The ports will remain part of the Marketing VLAN until reassigned to another VLAN.
   E. The ports were released from the Marketing VLAN and automatically reassigned to VLAN 1.

5. Which three statements are true about hosts configured in the same VLAN? (Choose three.)

   A. Hosts in the same VLAN must be on the same IP subnet.
   B. Hosts in different VLANs can communicate with the aid of only the Layer 2 switch.
   C. Hosts in the same VLAN share the same broadcast domain.
   D. Hosts in the same VLAN share the same collision domain.
   E. Hosts in the same VLAN comply with the same security policy.
   F. Hosts in the same VLAN must be on the same physical segment.

6. Refer to Figure 3-34. Host C is unable to transfer data because it does not have the MAC address of the destination host. If Host C sends out an ARP request, which of the other hosts will see the message?

Figure 3-34 LAN Connectivity



   A. Host A
   B. Host B
   C. Hosts A and B
   D. Hosts A and D
   E. Hosts B and D
   F. Hosts A, B, and D

7. With each listed VLAN characteristic on the right, indicate in the blank on the left whether it is a static VLAN characteristic or a dynamic VLAN characteristic. Use S for static and D for dynamic.

   ____ Each port associated with specific VLAN.
   ____ Manual configuration of port assignment required.
   ____ Ports work out their own configuration.
   ____ Less administrative overhead when users moved.
   ____ Requires administrator interaction when users moved.
   ____ Configured based on database.

8. With each listed characteristic on the right, indicate in the blank on the left whether it reflects a normal range VLAN, an extended range VLAN, or VLAN 1. Use N for normal range VLAN, E for extended range VLAN, and 1 for VLAN 1.

    ____ 1–1001

    ____ 1006–4094

    ____ Not learned by VTP

    ____ Stored in vlan.dat

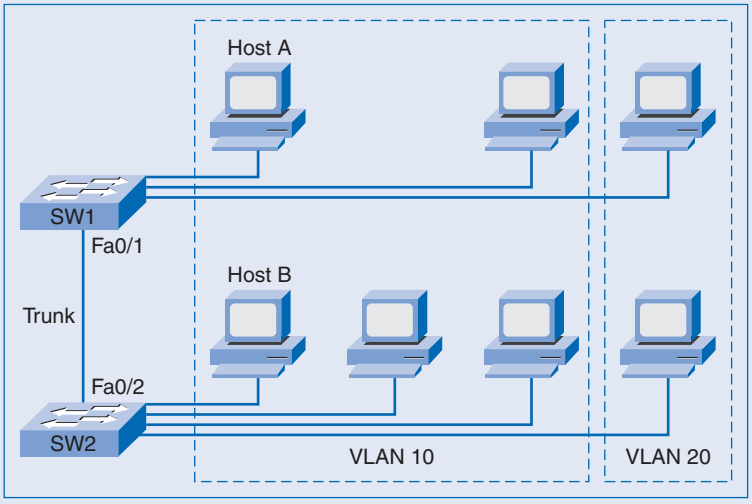
    ____ Default management VLAN

    ____ Default native VLAN

    ____ All ports are a member of by default

9. Refer to Figure 3-35. Brand new switches with empty MAC address tables are interconnected via a trunk link. All hosts on both switches are configured with the VLAN memberships shown. How is a frame sent from Host A forwarded to Host B?

Figure 3-35 Frame Flow



A. Switch SW1 floods the message from Host A to all hosts attached to SW1 that are members of VLAN 10.

B. Switch SW1 floods the message from Host A to all hosts attached to SW1.

C. Switch SW1 floods the message from Host A to all hosts attached to both switches.

D. Switch SW1 tags the frame with VLAN ID 10, and the frame is then flooded to all hosts on switch SW2 that are members of VLAN 10.

E. Switch SW1 tags the frame with VLAN ID 10, and the frame is then flooded to all hosts on switch SW2.

10. Refer to Example 3-29. Host 1 is connected to interface F0/4 with IP address 192.168.1.22/28. Host 2 is connected to interface F0/5 with IP address 192.168.1.33/28. Host 3 is connected to interface F0/6 with IP address 192.168.1.30/28. Select the three statements that describe the success of pinging from one host to another. (Choose three.)

Example 3-29 Connectivity After VLAN Configuration

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Accounting
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name Marketing
Switch(config-vlan)# interface range f0/4 , f0/6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# interface f0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

A. Host 1 can ping Host 2.

B. Host 1 cannot ping Host 2.

C. Host 1 can ping Host 3.

D. Host 1 cannot ping Host 3.

E. Host 2 can ping Host 3.

F. Host 2 cannot ping Host 3.

11. Which three options accurately associate the Catalyst switch command with the result? (Choose three.)

A. **show vlan id** *vlan-id*: displays information about a specific VLAN.

B. **show vlan**: displays detailed information about all VLANs on the switch.

C. **show vlan brief**: displays detailed information about all VLANs on the switch.

D. **show interface f0/1 switchport**: displays information about a specific port.

E. **show interface f0/1**: displays VLAN information about a specific port.

12. Match the commands with the correct descriptions.

____ **switchport mode trunk**

____ **switchport mode dynamic desirable**

____ **switchport nonegotiate**

____ **switchport mode access**

A. Configures the port to negotiate a trunk
B. Configures the trunk to not send DTP packets
C. Configures the port as a permanent 802.1Q trunk
D. Disables trunk mode

13. Match the problem definition with the correct problem description.

____ Native VLAN mismatch
____ Trunk mode mismatch
____ Incorrect VLAN list
____ VLAN subnet conflict

A. Both switches are configured to dynamic auto and will not negotiate a link.
B. Not all the VLANs needed are allowed to traverse a trunk.
C. Two VLANs are sharing the same address space.
D. The VLAN configured for untagged frames is not the same on two switches connected by a trunk.

14. Which three options accurately associate the static, dynamic, or voice VLAN membership with the port membership statement? (Choose three.)

A. Static VLAN port membership: port on a switch that can change the manually assigned VLAN configuration dynamically
B. Static VLAN port membership: port on a switch that maintains its assigned VLAN configuration until it is changed manually
C. Dynamic VLAN port membership: port on a switch using VMPS and associating a port to a VLAN based on the destination MAC address
D. Dynamic VLAN port membership: port on a switch using VMPS and associating a port to a VLAN based on the source MAC address
E. Voice VLAN port membership: access port attached to a PC, configured to use one VLAN for voice traffic and another VLAN for data traffic
F. Voice VLAN port membership: access port attached to an IP phone, configured to use one VLAN for voice traffic and another VLAN for data traffic

Challenge Questions and Activities

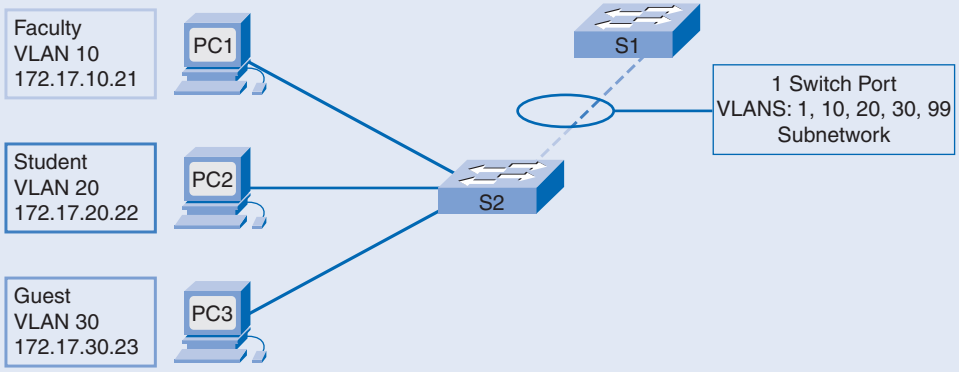
These questions require a deeper application of the concepts covered in this chapter. You can find the answers in the Appendix.

1. Which of the following best describes the mapping between VLANs and IP subnets in a modern switched network?

A. One IP subnet to many VLANs
B. One VLAN to many IP subnets
C. Two IP subnets to one VLAN
D. Two VLANs to one IP subnet
E. One IP subnet to one VLAN
F. Varies with the model of Cisco Catalyst switch

2. Refer to Figure 3-36. The dashed line indicates a trunk link. S1 and S2 are members of VLAN 99. Which two of the following are true? (Choose two.)

Figure 3-36 LAN Connectivity



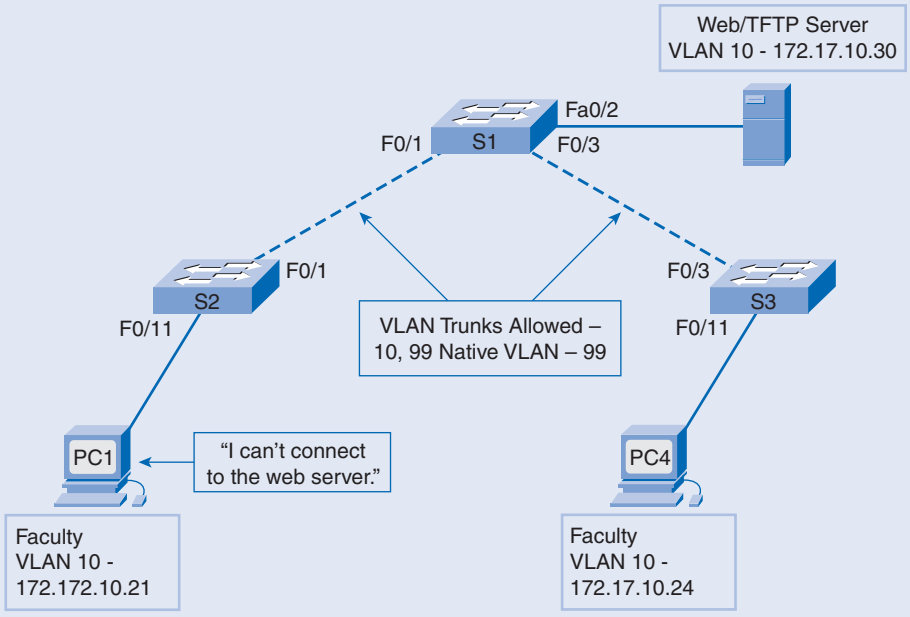
A. All PCs can successfully ping each other.
B. No PC can successfully ping another PC.
C. Switch S1 can successfully ping switch S2.
D. All the PCs can successfully ping switch S1.
E. All the PCs can successfully ping switch S2.

3. Which of the following is normally performed at the `Switch(config-vlan)#` prompt?

A. Addition of VLANs
B. Deletion of VLANs
C. Assignment of ports to VLANs
D. Naming of VLANs
E. Assignment of the native VLAN

4. Refer to Figure 3-37. What are some of the possible causes of the lack of connectivity?

Figure 3-37 Lack of Connectivity



A. Native VLAN mismatch on the trunk between switch S1 and switch S2.

B. Trunk mode mismatch between switch S1 and switch S2.

C. Misconfigured set of allowed VLANs on trunk between switch S1 and switch S2.

D. Misconfigured IP addresses associated with VLAN 10.

E. A link is down along the path between PC1 and the web/TFTP server.

Packet Tracer Challenge

Look for this icon in *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide*, (ISBN 1-58713-202-8) for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.