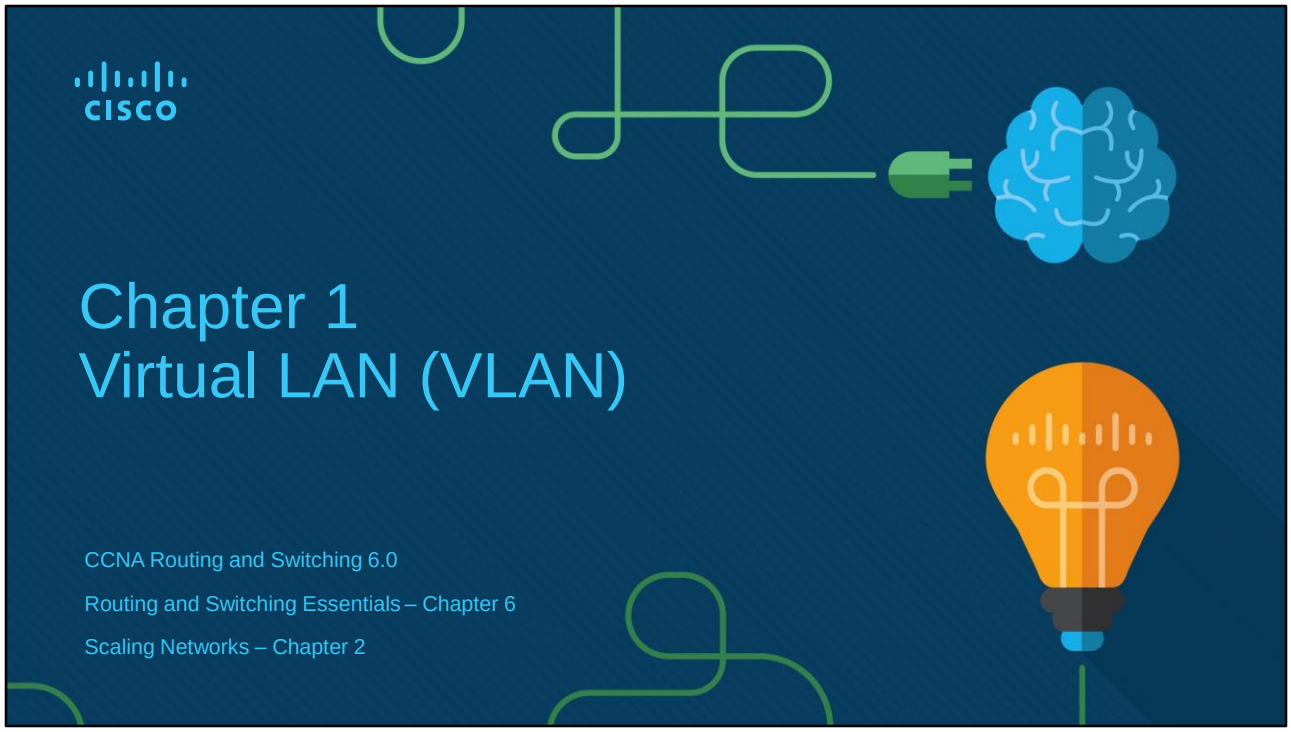

cisco
Chapter 1
Virtual LAN (VLAN)
CCNA Routing and Switching 6.0
Routing and Switching Essentials – Chapter 6
Scaling Networks – Chapter 2

Chapter 1 - Sections & Objectives

- VLAN Segmentation
  - Explain the purpose of VLANs in a switched network.
  - Explain how a switch forwards frames based on VLAN configuration in a multi-switch environment.
- Inter-VLAN Routing Using Routers
  - Describe the two options for configuring Inter-VLAN routing.
  - Configure legacy Inter-VLAN Routing.
  - Configure Router-on-a-Stick Inter-VLAN Routing
- Layer 3 Switching
  - Implement inter-VLAN routing using Layer 3 switching to forward data in a small to medium-sized business LAN.
    - Configure inter-VLAN routing using Layer 3 switching.
    - Troubleshoot inter-VLAN routing in a Layer 3 switched environment.

Chapter 6: VLANs

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

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

Because VLANs segment the network, a Layer 3 process is required to allow traffic to move from one network segment to another.

This Layer 3 routing process can either be implemented using a router or a Layer 3 switch interface. The use of a Layer 3 device provides a method for controlling the flow of traffic between network segments, including network segments created by VLANs.

The first part of this chapter will cover how to configure, manage, and troubleshoot VLANs and VLAN trunks. The second part of this chapter focuses on implementing

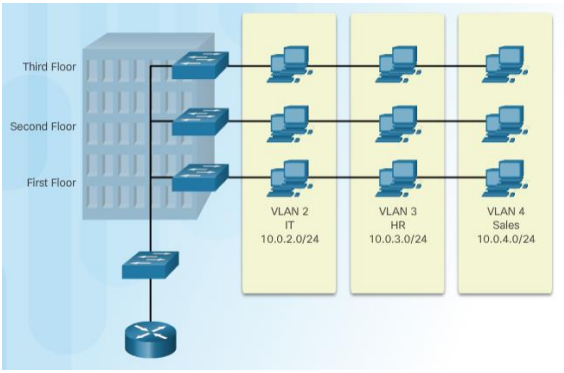
inter-VLAN routing using a router. Inter-VLAN routing on a Layer 3 switch is covered in a later course.

VLAN Segmentation

Overview of VLANs

VLAN Definitions

- VLANs can segment LAN devices without regard for the physical location of the user or device.
  - In the figure, IT users on the first, second, and third floors are all on the same LAN segment. The same is true for HR and Sales users.
- A VLAN is a logical partition of a Layer 2 network.
  - Multiple partitions can be created and multiple VLANs can co-exist.
  - The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.
  - Each VLAN is a broadcast domain that can span multiple physical LAN segments.
  - Hosts on the same VLAN are unaware of the VLAN's existence.



- VLANs are mutually isolated and packets can only pass between VLANs via a router.

VLAN Definitions

Within a switched network, VLANs provide segmentation and organizational flexibility. VLANs provide a way to group devices within a LAN. A group of devices within a VLAN communicate as if each device was attached to the same cable. VLANs are based on logical connections, instead of physical connections.

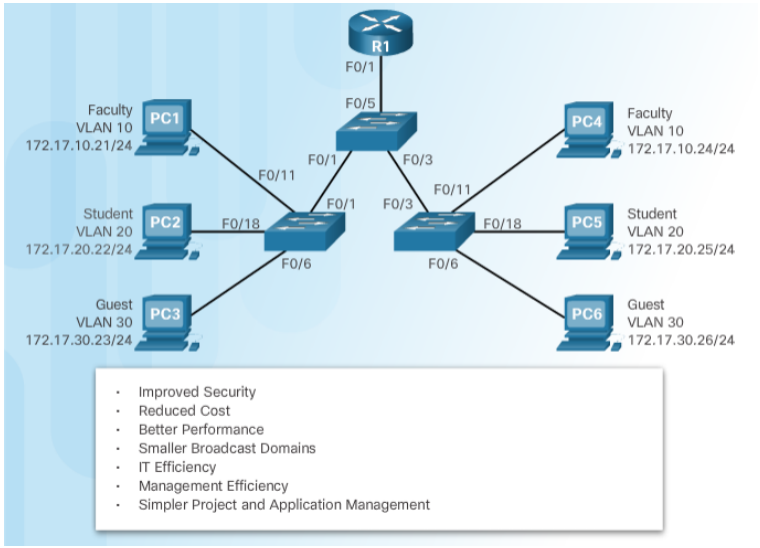
VLANs allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device. Each VLAN is considered a separate logical network. Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs. Any switch port can belong to a VLAN. Unicast, broadcast, and multicast packets are forwarded and flooded only to end devices within the VLAN where the packets are sourced. Packets destined for devices that do not belong to the VLAN must be forwarded through a device that supports routing. Multiple IP subnets can exist on a switched network, without the use of multiple VLANs. However, the devices will be in the same Layer 2 broadcast domain. This means that any Layer 2 broadcasts, such as an ARP request, will be received by all devices on the switched network, even by those not intended to receive the broadcast.

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

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

Overview of VLANs

Benefits of VLANs



Benefits of VLANs

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

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

Cost reduction - Cost savings result from reduced need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.

Better performance - Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces unnecessary traffic on the network and boosts performance.

Reduce the size of broadcast domains - Dividing a network into VLANs reduces the number of devices in the broadcast domain. As shown in the figure, there are six computers on this network but there are three broadcast domains: Faculty, Student, and Guest.

Improved IT staff efficiency - VLANs make it easier to manage the network because users with similar network requirements share the same VLAN. When a new switch is provisioned, all the policies and procedures already configured for the particular VLAN are implemented when the ports are assigned. It is also easy for the IT staff to identify the function of a VLAN by giving it an appropriate name. In the figure, for

easy identification VLAN 10 has been named “Faculty”, VLAN 20 is named “Student”, and VLAN 30 “Guest.”

Simpler project and application management - VLANs aggregate users and network devices to support business or geographic requirements. Having separate functions makes managing a project or working with a specialized application easier; an example of such an application is an e-learning development platform for faculty. Each VLAN in a switched network corresponds to an IP network. Therefore, VLAN design must take into consideration the implementation of a hierarchical network-addressing scheme. Hierarchical network addressing means that IP network numbers are applied to network segments or VLANs in an orderly fashion that takes the network as a whole into consideration. Blocks of contiguous network addresses are reserved for and configured on devices in a specific area of the network, as shown in the figure.

Overview of VLANs

Types of VLANs

- Common types of VLANs:
  - **Default VLAN** – Also known as VLAN 1. All switch ports are members of VLAN 1 by default.
  - **Data VLAN** – Data VLANs are commonly created for specific groups of users or devices. They carry user generated traffic.
  - **Native VLAN** – This is the VLAN that carries all untagged traffic. This is traffic that does not originate from a VLAN port (e.g., STP BPDU traffic exchanged between STP enabled switches). The native VLAN is VLAN 1 by default.
  - **Management VLAN** – This is a VLAN that is created to carry network management traffic including SSH, SNMP, Syslog, and more. VLAN 1 is the default VLAN used for network management.

Default VLAN Assignment

```
Switch# show vlan brief

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

Initially, all switch ports are members of VLAN 1.

Types of VLANs

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

Data VLAN

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

Default VLAN

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

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

Native VLAN

A native VLAN is assigned to an 802.1Q trunk port. Trunk ports are the links between

switches that support the transmission of traffic associated with more than one VLAN. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic), as well as traffic that does not come from a VLAN (untagged traffic). Tagged traffic refers to traffic that has a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs. The 802.1Q trunk port places untagged traffic on the native VLAN, which by default is VLAN 1.
Native VLANs are defined in the IEEE 802.1Q specification to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. A native VLAN serves as a common identifier on opposite ends of a trunk link.
It is a best practice to configure the native VLAN as an unused VLAN, distinct from VLAN 1 and other VLANs. In fact, it is not unusual to dedicate a fixed VLAN to serve the role of the native VLAN for all trunk ports in the switched domain.

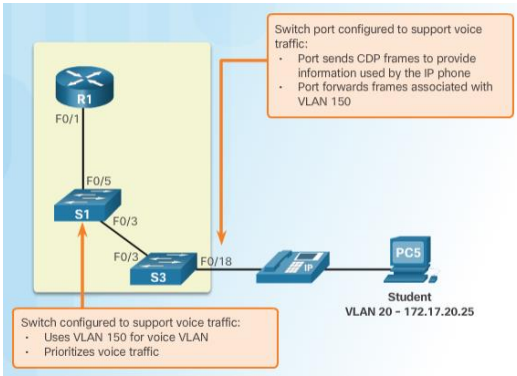
Management VLAN

A management VLAN is any VLAN configured to access the management capabilities of a switch. VLAN 1 is the management VLAN by default. To create the management VLAN, the switch virtual interface (SVI) of that VLAN is assigned an IP address and a subnet mask, allowing the switch to be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 would be a bad choice for the management VLAN.
In the past, the management VLAN for a 2960 switch was the only active SVI. On 15.x versions of the Cisco IOS for Catalyst 2960 Series switches, it is possible to have more than one active SVI. Cisco IOS 15.x requires that the particular active SVI assigned for remote management be documented. While theoretically a switch can have more than one management VLAN, having more than one increases exposure to network attacks.
In the figure, all ports are currently assigned to the default VLAN 1. No native VLAN is explicitly assigned and no other VLANs are active; therefore, the network is designed with the native VLAN the same as the management VLAN. This is considered a security risk.

Overview of VLANs

Voice VLANs

- To support time-sensitive voice traffic, some vender switches, namely Cisco, support a voice VLAN that requires:
  - Assured bandwidth
  - Delay of less than 150 ms across the network to ensure voice quality
  - Transmission priority over other types of network traffic
  - Ability to be routed around congested areas on the network.



- The voice VLAN feature enables access ports to carry user and IP voice traffic.
  - In the figure, the S3 F0/18 interface has been configured to tag student traffic on VLAN 20 and voice traffic on VLAN 150.

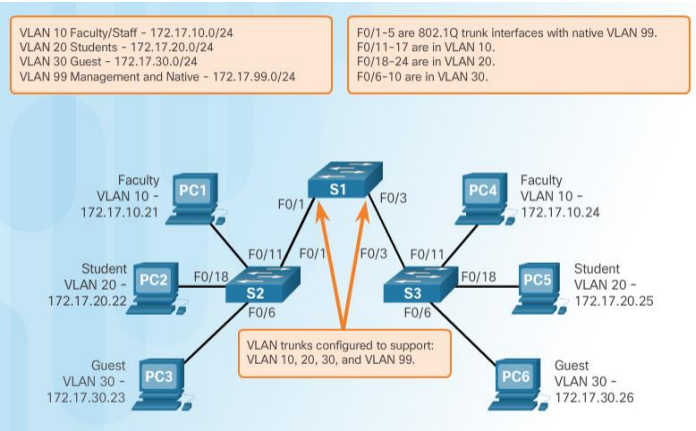
Voice VLANs

A separate VLAN is needed to support Voice over IP (VoIP). VoIP traffic requires:
Assured bandwidth to ensure voice quality
Transmission priority over other types of network traffic
Ability to be routed around congested areas on the network
Delay of less than 150 ms across the network
To meet these requirements, the entire network has to be designed to support VoIP.
In the figure, 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.

VLANs in a Multi-Switched Environment

VLAN Trunks

- A VLAN trunk is a point-to-point link that carries more than one VLAN.
  - Usually established between switches to support intra VLAN communication.
  - A VLAN trunk or trunk ports are not associated to any VLANs.
- Cisco IOS supports IEEE 802.1q, a popular VLAN trunk protocol.



The links between switches S1 and S2, and S1 and S3 are configured to transmit traffic coming from VLANs 10, 20, 30, and 99 across the network.

VLAN Trunks

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

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

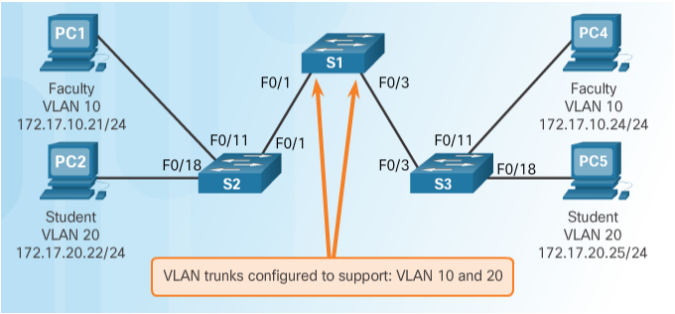
A VLAN trunk does not belong to a specific VLAN; rather, it is a conduit for multiple VLANs between switches and routers. A trunk could also be used between a network device and server or other device that is equipped with an appropriate 802.1Q-capable NIC. By default, on a Cisco Catalyst switch, all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

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

VLANs in a Multi-Switched Environment

Controlling Broadcast Domains with VLANs

- If a switch port receives a broadcast frame, it forwards it out all ports except the originating port.
  - Eventually the entire network receives the broadcast because the network is one broadcast domain.
- VLANs can be used to limit the reach of broadcast frames because each VLAN is a broadcast domain.
  - VLANs help control the reach of broadcast frames and their impact in the network.
- In the figure, PC1 on VLAN 10 sends a broadcast frame.
  - Trunk links between S2 - S1 and S1 - S3 propagate the broadcast to other devices in VLAN 10.
  - Only devices in the same VLAN receive the broadcast therefore, PC4 would receive the broadcast.



Controlling Broadcast Domains with VLANs

Network without VLANs

In normal operation, when a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports except the port where the broadcast was received. In the animation in Figure 1, the entire network is configured in the same subnet (172.17.40.0/24) and no VLANs are configured. As a result, when the faculty computer (PC1) sends out a broadcast frame, switch S2 sends that broadcast frame out all of its ports. Eventually the entire network receives the broadcast because the network is one broadcast domain.

In this example, all devices are on the same IPv4 subnet. If there were devices on other IPv4 subnets, they would also receive the same broadcast frame. Broadcasts such as an ARP request, are intended only for devices on the same subnet.

Network with VLANs

As shown in the animation in Figure 2, the network has been segmented using two VLANs. Faculty devices are assigned to VLAN 10 and student devices are assigned to VLAN 20. When a broadcast frame is sent from the faculty computer, PC1, to switch S2, the switch forwards that broadcast frame only to those switch ports configured to support VLAN 10.

The ports that comprise the connection between switches S2 and S1 (ports F0/1), and between S1 and S3 (ports F0/3) are trunks and have been configured to support all the VLANs in the network.

When S1 receives the broadcast frame on port F0/1, S1 forwards that broadcast

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

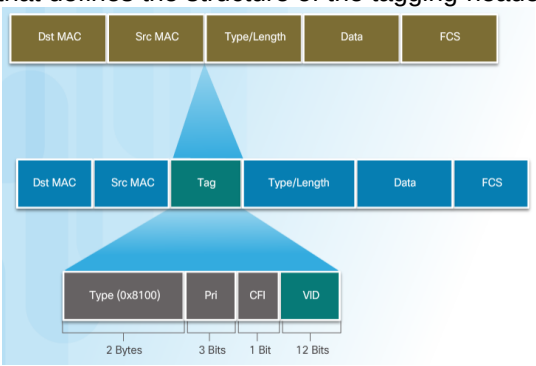
When VLANs are implemented on a switch, the transmission of unicast, multicast, and broadcast traffic from a host in a particular VLAN are restricted to the devices that are in that VLAN.

VLANs in a Multi-Switched Environment

Tagging Ethernet Frames for VLAN Identification

- Before a frame is forwarded across a trunk link, it must be tagged with its VLAN information.
  - Frame tagging is the process of adding a VLAN identification header to the frame.
  - It is used to properly transmit multiple VLAN frames through a trunk link.

- IEEE 802.1Q is a vey popular VLAN trunking protocol that defines the structure of the tagging header added to the frame.
  - Switches add VLAN tagging information after the Source MAC address field.
  - The fields in the 802.1Q VLAN tag includes VLAN ID (VID).
  - Trunk links add the tag information before sending the frame and then remove the tags before forwarding frames through non-trunk ports.



agging Ethernet Frames for VLAN Identification

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

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

VLAN Tag Field Details

The VLAN tag field consists of a Type field, a Priority field, a Canonical Format Identifier field, and VLAN ID field:

Type - A 2-byte value called the tag protocol ID (TPID) value. For Ethernet, it is set to hexadecimal 0x8100.

User priority - A 3-bit value that supports level or service implementation.

Canonical Format Identifier (CFI) - A 1-bit identifier that enables Token Ring frames to be carried across Ethernet links.

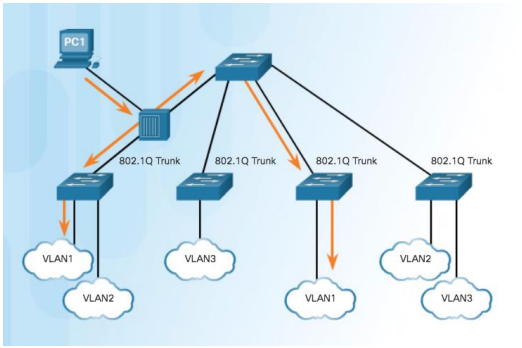
VLAN ID (VID) - A 12-bit VLAN identification number that supports up to 4096 VLAN IDs.

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

VLANs in a Multi-Switched Environment

Native VLANs and 802.1Q Tagging

- Control traffic sent on the native VLAN should not be tagged.
- Frames received untagged, remain untagged and are placed in the native VLAN when forwarded.
- If there are no ports associated to the native VLAN and no other trunk links, an untagged frame is dropped.
- When configuring a switch port on a Cisco switch, configure devices so that they do not send tagged frames on the native VLAN.
- In Cisco switches, the native VLAN is VLAN 1, by default.



Native VLANs and 802.1Q Tagging

Tagged Frames on the Native VLAN

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

Untagged Frames on the Native VLAN

When a Cisco switch trunk port receives untagged frames (which are unusual in a well-designed network), it forwards those frames to the native VLAN. If there are no devices associated with the native VLAN (which is not unusual) and there are no other trunk ports (which is not unusual), then the frame is dropped. The default native VLAN is VLAN 1. When configuring an 802.1Q trunk port, a default Port VLAN ID (PVID) is assigned the value of the native VLAN ID. All untagged traffic coming 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.

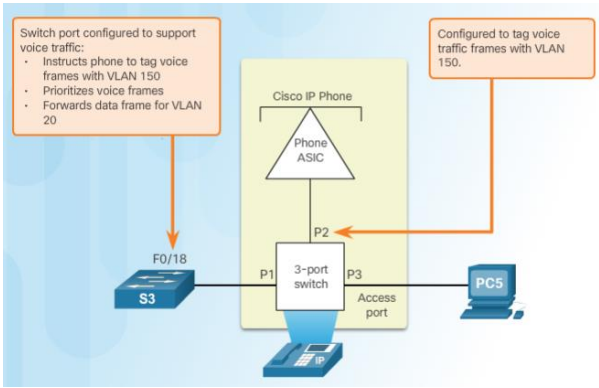
In the figure, PC1 is connected by a hub to an 802.1Q trunk link. PC1 sends untagged traffic, which the switches associate with the native VLAN configured on the trunk

ports, and forward accordingly. Tagged traffic on the trunk received by PC1 is dropped. This scenario reflects poor network design for several reasons: it uses a hub, it has a host connected to a trunk link, and it implies that the switches have access ports assigned to the native VLAN. It also illustrates the motivation for the IEEE 802.1Q specification for native VLANs as a means of handling legacy scenarios.

VLANs in a Multi-Switched Environment

Voice VLAN Tagging

- An access port connecting a Cisco IP phone can be configured to use two separate VLANs:
  - A VLAN for voice traffic
  - A VLAN for data traffic from a device attached to the phone.
- The link between the switch and the IP phone behaves like a trunk to carry traffic from both VLANs.



- Cisco IP Phone contains an integrated three-port 10/100 switch dedicated 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.

Voice VLAN Tagging

A separate voice VLAN is required to support VoIP.

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

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

Port 1 connects to the switch or other VoIP device.

Port 2 is an internal 10/100 interface that carries the IP phone traffic.

Port 3 (access port) connects to a PC or other device.

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

In a voice VLAN tagged with a Layer 2 class of service (CoS) priority value

In an access VLAN tagged with a Layer 2 CoS priority value

In an access VLAN, untagged (no Layer 2 CoS priority value)

In Figure 1, the student computer PC5 is attached to a Cisco IP phone, and the phone is attached to switch S3. VLAN 150 is designed to carry voice traffic, while PC5 is in VLAN 20, which is used for student data.

Sample Configuration

Figure 2 shows a sample output. A discussion of voice Cisco IOS commands are

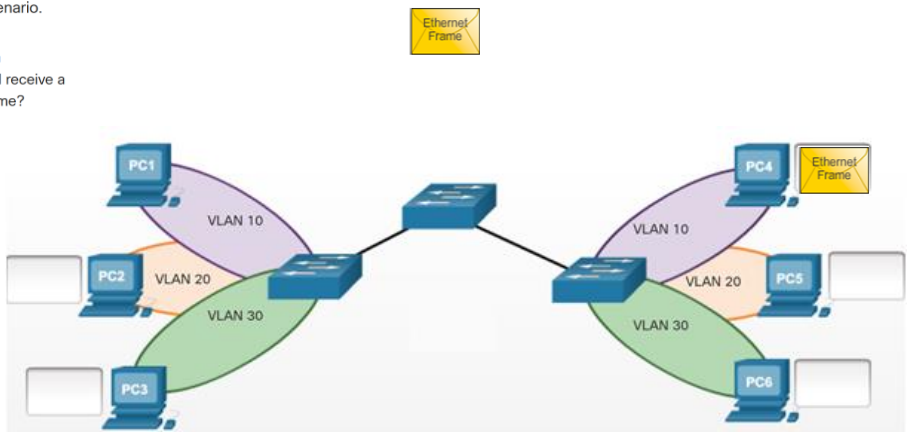
beyond the scope of this course, but the highlighted areas in the sample output show the F0/18 interface configured with a VLAN configured for data (VLAN 20) and a VLAN configured for voice (VLAN 150).

VLANs in a Multi-Switched Environment

Activity – VLAN trunk in action

Drag the Ethernet Frames (yellow envelopes) to their destination PCs for the scenario. Not all envelopes will be used in every scenario.

Scenario 1: PC 1 sends a broadcast. Which PCs will receive a copy of the broadcast frame?



Voice VLAN Tagging

A separate voice VLAN is required to support VoIP.

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

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

Port 1 connects to the switch or other VoIP device.

Port 2 is an internal 10/100 interface that carries the IP phone traffic.

Port 3 (access port) connects to a PC or other device.

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

In a voice VLAN tagged with a Layer 2 class of service (CoS) priority value

In an access VLAN tagged with a Layer 2 CoS priority value

In an access VLAN, untagged (no Layer 2 CoS priority value)

In Figure 1, the student computer PC5 is attached to a Cisco IP phone, and the phone is attached to switch S3. VLAN 150 is designed to carry voice traffic, while PC5 is in VLAN 20, which is used for student data.

Sample Configuration

Figure 2 shows a sample output. A discussion of voice Cisco IOS commands are

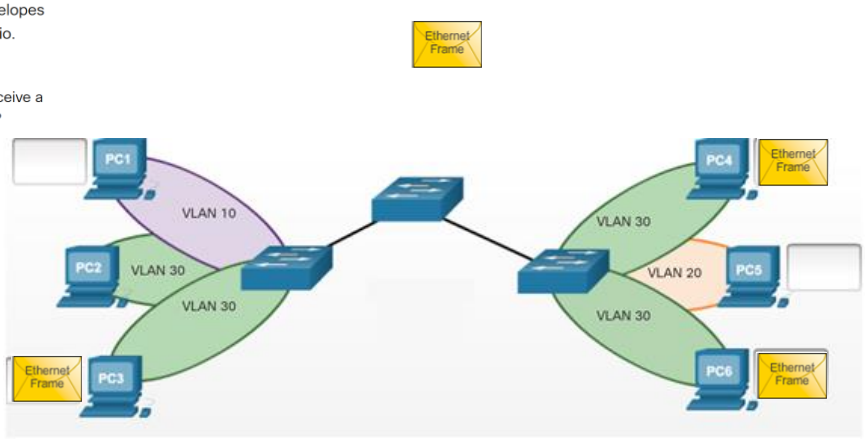
beyond the scope of this course, but the highlighted areas in the sample output show the F0/18 interface configured with a VLAN configured for data (VLAN 20) and a VLAN configured for voice (VLAN 150).

VLANs in a Multi-Switched Environment

Activity – VLAN trunk in action

Drag the Ethernet Frames (yellow envelopes) to their destination PCs for the scenario. Not all envelopes will be used in every scenario.

Scenario 2: PC 2 sends a broadcast. Which PCs will receive a copy of the broadcast frame?



Voice VLAN Tagging

A separate voice VLAN is required to support VoIP.

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

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

Port 1 connects to the switch or other VoIP device.

Port 2 is an internal 10/100 interface that carries the IP phone traffic.

Port 3 (access port) connects to a PC or other device.

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

In a voice VLAN tagged with a Layer 2 class of service (CoS) priority value

In an access VLAN tagged with a Layer 2 CoS priority value

In an access VLAN, untagged (no Layer 2 CoS priority value)

In Figure 1, the student computer PC5 is attached to a Cisco IP phone, and the phone is attached to switch S3. VLAN 150 is designed to carry voice traffic, while PC5 is in VLAN 20, which is used for student data.

Sample Configuration

Figure 2 shows a sample output. A discussion of voice Cisco IOS commands are

beyond the scope of this course, but the highlighted areas in the sample output show the F0/18 interface configured with a VLAN configured for data (VLAN 20) and a VLAN configured for voice (VLAN 150).

6.2 VLAN Implementation

VLAN Assignment

VLAN Ranges on Catalyst Switches

- VLANs are split into two categories:
  - **Normal range VLANs**
    - VLAN numbers from 1 to 1,005
    - Configurations stored in the vlan.dat (in the flash memory)
    - IDs 1002 through 1005 are reserved for legacy Token Ring and Fiber Distributed Data Interface (FDDI) VLANs, automatically created and cannot be removed.
  - **Extended Range VLANs**
    - VLAN numbers from 1,006 to 4,096
    - Configurations stored in the running configuration (NVRAM)
    - VLAN Trunking Protocol (VTP) does not learn extended VLANs

- Cisco Catalyst 2960 and 3560 Series switches support over 4,000 VLANs.

```
Switch# show vlan brief

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


VLAN Ranges on Catalyst Switches

Different Cisco Catalyst switches support various numbers of VLANs. The number of supported VLANs is large enough to accommodate the needs of most organizations. For example, the Catalyst 2960 and 3560 Series switches support over 4,000 VLANs. Normal range VLANs on these switches are numbered 1 to 1,005 and extended range VLANs are numbered 1,006 to 4,094. The figure illustrates the available VLANs on a Catalyst 2960 switch running Cisco IOS Release 15.x.

Normal Range VLANs

Used in small- and medium-sized business and enterprise networks.

Identified by a VLAN ID between 1 and 1005.

IDs 1002 through 1005 are reserved for Token Ring and Fiber Distributed Data Interface (FDDI) VLANs.

IDs 1 and 1002 to 1005 are automatically created and cannot be removed.

Configurations are stored within a VLAN database file, called vlan.dat. The vlan.dat file is located in the flash memory of the switch.

The VLAN Trunking Protocol (VTP), which helps manage VLAN configurations between switches, can only learn and store normal range VLANs.

Extended Range VLANs

Enable service providers to extend their infrastructure to a greater number of customers. Some global enterprises could be large enough to need extended range VLAN IDs.

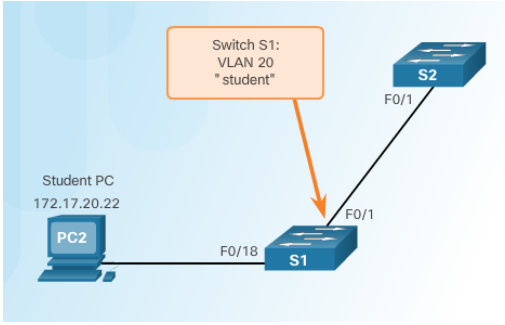
Are identified by a VLAN ID between 1006 and 4094.

Configurations are not written to the vlan.dat file.
Support fewer VLAN features than normal range VLANs.
Saved, by default, in the running configuration file.
VTP does not learn extended range VLANs.
Note: 4096 is the upper boundary for the number of VLANs available on Catalyst switches, because there are 12 bits in the VLAN ID field of the IEEE 802.1Q header.

VLAN Assignment

Creating a VLAN

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




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


Creating a VLAN

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

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

Figure 2 shows how the student VLAN (VLAN 20) is configured on switch S1. In the topology example, the student computer (PC2) has not been associated with a VLAN yet, but it does have an IP address of 172.17.20.22.

Use the Syntax Checker in Figure 3 to create a VLAN and use the **show vlan brief** command to display the contents of the vlan.dat file.

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

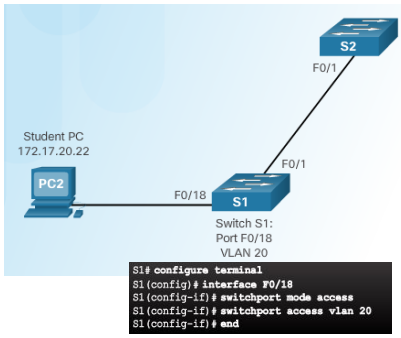
S1(config)# **vlan 100,102,105-107**

VLAN Assignment

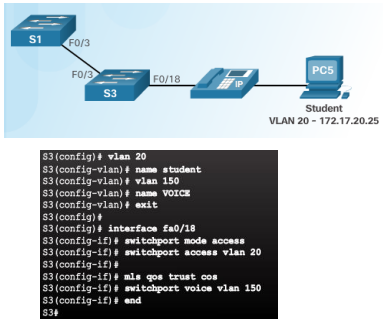
Assigning Ports to VLANs

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

Example 1



Example 2



Assigning Ports to VLANs

After creating a VLAN, the next step is to assign ports to the VLAN.

Figure 1 displays the syntax for defining a port to be an access port and assigning it to a VLAN. The **switchport mode access** command is optional, but strongly recommended as a security best practice. With this command, the interface changes to permanent access mode.

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

In the example in Figure 2, VLAN 20 is assigned to port F0/18 on switch S1. Any device connected to that port is associated with VLAN 20. Therefore, in our example, PC2 is in VLAN 20.

It is important to note that VLANs are configured on the switch port and not on the end device. PC2 is configured with an IPv4 address and subnet mask that is associated with the VLAN, which is configured on the switch port. In this example, it is VLAN 20. When VLAN 20 is configured on other switches, the network administrator must configure the other student computers to be in the same subnet as PC2 (172.17.20.0/24).

An access port can belong to only one VLAN at a time. However, one exception to this rule is that of a port connected to an IP phone and an end device. In this case, there would be two VLANs associated with the port: one for voice and one for data.

Consider the topology in Figure 3. In this example, PC5 is connected to the Cisco IP phone, which in turn is connected to the FastEthernet 0/18 interface on S3. To

implement this configuration, VLAN 20 and the voice VLAN 150 are created.
Use the **switchport voice vlan** *vlan-#* interface configurationcommandto assign a voice VLAN to a port.
LANs supporting voice traffic typically also have Quality of Service (QoS) enabled. Voice traffic must be labeled as trusted as soon as it enters the network. Use the **mls qos trust[cos | device cisco-phone | dscp | ip-precedence]** interface configuration command to set the trusted state of an interface, and to indicate which fields of the packet are used to classify traffic.
The configuration in Figure 4 creates the two VLANs (i.e., VLAN 20 and VLAN 150) and then assigns the F0/18 interface of S3 as a switchport in VLAN 20. It also assigns voice traffic to VLAN 150 and enables QoS classification based on the class of service (CoS) assigned by the IP phone.
Note: The implementation of QoS is beyond the scope of this course. Refer to cisco.com for more information.
Use the Syntax Checker in Figure 5 to assign a data VLAN and voice VLAN. You will also use the **show vlan brief** command to display the contents of the vlan.dat file.
The **switchport access vlan** command forces the creation of a VLAN if it does not already exist on the switch. For example, VLAN 30 is not present in the **show vlan brief** output of the switch. If the **switchport access vlan 30** command is entered on any interface with no previous configuration, then the switch displays the following:
% Access VLAN does not exist. Creating vlan 30

VLAN Assignment

Changing VLAN Port Membership

- Remove VLAN Assignment

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode	S1(config)# interface F0/18
Remove the VLAN assignment from the port.	S1(config-if)# no switchport access vlan
Return to the privileged EXEC mode.	S1(config-if)# end

Even though interface F0/18 was previously assigned to VLAN 20, it reset to the default VLAN1.

```
S1(config)# int 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#
```

Changing VLAN Port Membership

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

Interface F0/18 was previously assigned to VLAN 20. The **no switchport access vlan** command is entered for interface F0/18. Examine the output in the **show vlan brief** command that immediately follows, as shown in Figure 2. The **show vlan brief** command displays the VLAN assignment and membership type for all switch ports. The **show vlan brief** command displays one line for each VLAN. The output for each VLAN includes the VLAN name, status, and switch ports.

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

A port can easily have its VLAN membership changed. It is not necessary to first remove a port from a VLAN to change its VLAN membership. When an access port has its VLAN membership reassigned to another existing VLAN, the new VLAN membership simply replaces the previous VLAN membership. In Figure 4, port F0/11 is assigned to VLAN 20.

Use the Syntax Checker in Figure 5 to change VLAN port membership.

VLAN Assignment

Deleting VLANs

- Use the **no vlan** *vlan-id* global configuration mode command to remove VLAN.

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh 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
S1#
```

- To delete the entire vlan.dat file, use the **delete flash:vlan.dat** privileged EXEC mode command.
  - **delete vlan.dat** can be used if the vlan.dat file has not been moved from its default location.

Deleting VLANs

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

Caution: Before deleting a VLAN, reassign all member ports to a different VLAN first. Any ports that are not moved to an active VLAN are unable to communicate with other hosts after the VLAN is deleted and until they are assigned to an active VLAN. Alternatively, the entire vlan.dat file can be deleted using the **delete flash:vlan.dat** privileged EXEC mode command. The abbreviated command version (**delete vlan.dat**) can be used if the vlan.dat file has not been moved from its default location. After issuing this command and reloading the switch, the previously configured VLANs are no longer present. This effectively places the switch into its factory default condition with regard to VLAN configurations.

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

VLAN Assignment

Verifying VLAN Information

- VLAN configurations can be validated using the Cisco IOS **show vlan** and **show interfaces** command options.

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, 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
------- --------- ----------------- ------------------------

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

S1#
```

```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia 001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 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
```


Verifying VLAN Information

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

Figure 1 displays the **show vlan** and **show interfaces** command options.

In the example in Figure 2, the **show vlan name student** command produces output that is not easily interpreted. The **show vlan summary** command displays the count of all configured VLANs. The output in Figure 2 shows seven VLANs.

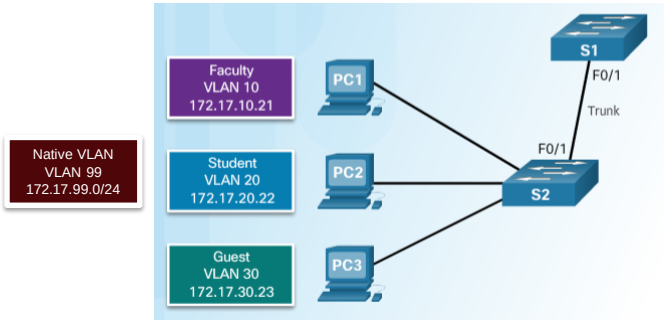
The **show interfaces vlan** *vlan-id* command displays details that are beyond the scope of this course. The important information appears on the second line in Figure 3, indicating that VLAN 20 is up.

Use the Syntax Checker in Figure 4 to display the VLAN and switch port information, and to verify VLAN assignments and mode.

VLAN Trunks

Configuring IEEE 802.1q Trunk Links

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




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


Configuring IEEE 802.1Q Trunk Links

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

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

Note: DTP is beyond the scope of this course.

The Cisco IOS command syntax to specify a native VLAN (other than VLAN 1) is shown in Figure 1. In the example, VLAN 99 is configured as the native VLAN using the **switchport trunk native vlan 99** command.

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

In Figure 2, VLANs 10, 20, and 30 support the Faculty, Student, and Guest computers (PC1, PC2, and PC3). The F0/1 port on switch S1 is configured as a trunk port and forwards traffic for VLANs 10, 20, and 30. VLAN 99 is configured as the native VLAN. Figure 3 displays the configuration of port F0/1 on switch S1 as a trunk port. The native VLAN is changed to VLAN 99 and the allowed VLAN list is restricted to 10, 20,

30, and 99.

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

VLAN Trunks

Resetting the Trunk to Default State

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface** *interface_id*
Set trunk to allow all VLANs.	S1(config-if)# **no switchport trunk allowed vlan**
Reset native VLAN to default.	S1(config-if)# **no switchport trunk native vlan**
Return to the privileged EXEC mode.	S1(config-if)# **end**

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

F0/1 is configured as an access port which removes the trunk feature.

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


Resetting the Trunk to Default State

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

Figure 2 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.

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

VLAN Trunks

Verifying Trunk Configuration

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


Verifying Trunk Configuration

Figure 1 displays the configuration of switch port F0/1 on switch S1. The configuration is verified with the **show interfaces** *interface-ID* **switchport** command.

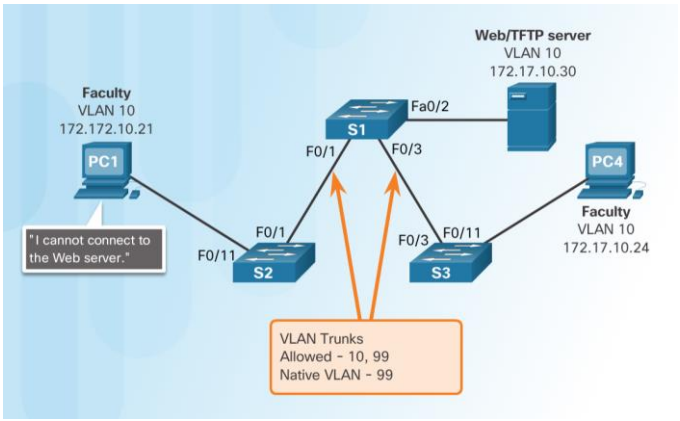
The top highlighted area shows that port F0/1 has its administrative mode set to **trunk**. The port is in trunking mode. The next highlighted area verifies that the native VLAN is VLAN 99. Further down in the output, the bottom highlighted area shows that all VLANs are enabled on the trunk.

Use the Syntax Checker in Figure 2 to configure a trunk supporting all VLANs on interface F0/1, with native VLAN 99. Verify the trunk configuration with the **show interfaces f0/1 switchport** command.

Troubleshoot VLANs and Trunks

IP Addressing Issues with VLANs

- Common practice to associate a VLAN with an IP network.
  - Different IP networks must communicate through a router.
  - All devices within a VLAN must be part of the same IP network to communicate.
- In the figure, PC1 cannot communicate to the server because it has a wrong IP address configured.



IP Addressing Issues with VLAN

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

In Figure 1, PC1 cannot connect to the Web/TFTP server shown.

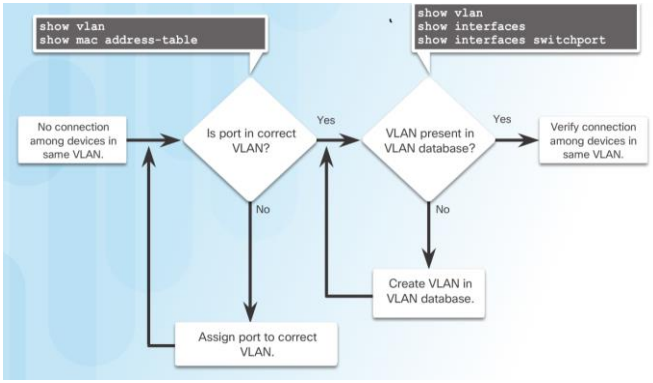
A check of the IPv4 configuration settings of PC1 shown in Figure 2, reveals the most common error in configuring VLANs: an incorrectly configured IPv4 address. PC1 is configured with an IPv4 address of 172.172.10.21, but it should have been configured with 172.17.10.21.

In Figure 3, the PC1 Fast Ethernet configuration dialog box shows the updated IPv4 address of 172.17.10.21. The output on the bottom reveals that PC1 has regained connectivity to the Web/TFTP server found at IPv4 address 172.17.10.30.

Troubleshoot VLANs and Trunks

Missing VLANs

- If all the IP address mismatches have been solved, but the device still cannot connect, check if the VLAN exists in the switch.



If the VLAN to which the port belongs is deleted, the port becomes inactive and is unable to communicate with the rest of the network.

- It is not functional until the missing VLAN is created or the VLAN is removed from the port.

```
S1# show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```


Missing VLANs

If there is still no connection between devices in a VLAN, but IP addressing issues have been ruled out, refer to the flowchart in Figure 1 to troubleshoot:

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

Step 2. If the VLAN to which the port is assigned is deleted, the port becomes inactive. The ports of a deleted VLAN will not be listed in the output of the **show vlan** command. Use the **show interfaces switchport** command to verify the inactive VLAN is assigned to the port, as shown in Figure 2.

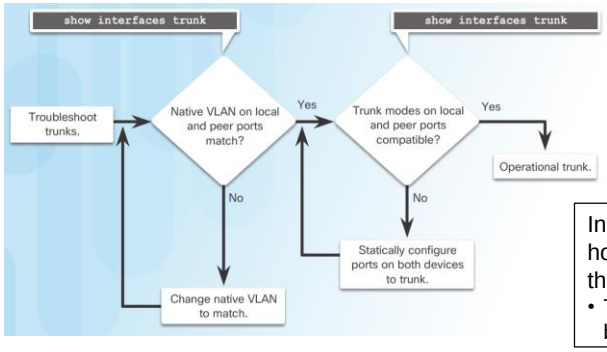
The example in Figure 2 shows MAC addresses that were learned on the F0/1 interface. It can be seen that MAC address 000c.296a.a21c was learned on interface F0/1 in VLAN 10. If this number is not the expected VLAN number, change the port VLAN membership using the **switchport access vlan** command.

Each port in a switch belongs to a VLAN. If the VLAN to which the port belongs is deleted, the port becomes inactive. All ports belonging to the VLAN that was deleted are unable to communicate with the rest of the network. Use the **show interface f0/1 switchport** command to check whether the port is inactive. If the port is inactive, it is not functional until the missing VLAN is created using the **vlan** *vlan-id* global configuration command or the VLAN is removed from the port with the **no**

switchport access vlan *vlan-id* command.

Troubleshoot VLANs and Trunks

Introduction to Troubleshooting Trunks



In this example, the Native VLAN should be VLAN 99 however, the output of the command identifies VLAN 2 as the Native VLAN.

- To solve this problem, configure the same native VLAN on both sides.

```
SW1# show interfaces f0/1 trunk

Port        Mode     Encapsulation  Status      Native vlan
Fa0/1       auto     802.1q         trunking    2

<output omitted>
```


Introduction to Troubleshooting Trunks

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

Figure 1 displays a flowchart of general trunk troubleshooting guidelines.

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

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

Step 2. Use the **show interfaces trunk** command to check whether a trunk has been established between switches. Statically configure trunk links whenever possible. Cisco Catalyst switch ports use DTP by default and attempt to negotiate a trunk link. To display the status of the trunk, the native VLAN used on that trunk link, and verify trunk establishment, use the **show interfaces trunk** command. The example in Figure 2 shows that the native VLAN on one side of the trunk link was changed to VLAN 2. If one end of the trunk is configured as native VLAN 99 and the other end is configured as native VLAN 2, a frame sent from VLAN 99 on one side is received on VLAN 2 on the other side. VLAN 99 leaks into the VLAN 2 segment.

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

message:
*Mar 1 06:45:26.232: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).
Connectivity issues occur in the network if a native VLAN mismatch exists. Data traffic for VLANs, other than the two native VLANs configured, successfully propagates across the trunk link, but data associated with either of the native VLANs does not successfully propagate across the trunk link.
As shown in Figure 2, native VLAN mismatch issues do not keep the trunk from forming. To solve the native VLAN mismatch, configure the native VLAN to be the same VLAN on both sides of the link.

Troubleshoot VLANs and Trunks

Common Problems with Trunks

- Trunking issues are usually associated with incorrect configurations.
- The most common type of trunk configuration errors are:

Problem	Result	Example
Native VLAN Mismatches	Poses a security risk and creates unintended results.	For example, one port is defined as VLAN 99 and the other is defined as VLAN 100.
Trunk Mode Mismatches	Causes loss of network connectivity.	For example, one side of the trunk is configured as an access port.
Allowed VLANs on Trunks	Causes unexpected traffic or no traffic to be sent over the trunk.	The list of allowed VLANs does not support current VLAN trunking requirements.

- When a trunk problem is suspected, it is recommended to troubleshoot in the order shown above.

Common Problems with Trunks

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

Native VLAN mismatches - Trunk ports are configured with different native VLANs. This configuration error generates console notifications, and can cause inter-VLAN routing issues, among other problems. This poses a security risk.

Trunk mode mismatches - One trunk port is configured in a mode that is not compatible for trunking on the corresponding peer port. This configuration error causes the trunk link to stop working. Be sure both sides of the trunk are configured with the **switchport mode trunk** command. Other trunk configuration commands are beyond the scope of this course.

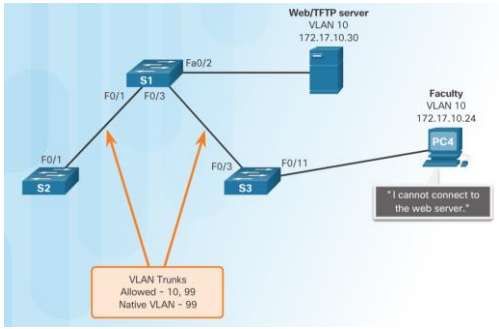
Allowed VLANs on trunks - The list of allowed VLANs on a trunk has not been updated with the current VLAN trunking requirements. In this situation, unexpected traffic (or no traffic) is being sent over the trunk.

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

Troubleshoot VLANs and Trunks

Incorrect Port Mode

- In this example, PC4 cannot reach the Web server.
  - The trunk links on S1 and S3 are verified and reveal that the S3 trunk port has been configured as an access port.




```
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: trunk
```

```
S3# show interfaces trunk

S3#
S3# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
…
```

To resolve the issue, the S3 F03 port is configured as a trunk link.

```
S3# config terminal
S3(config)# interface f0/3
S3(config-if)# switchport mode trunk
S3(config-if)# end
```


Incorrect Port Mode

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

In the scenario illustrated in Figure 1, PC4 cannot connect to the internal web server. The topology indicates a valid configuration. Why is there a problem?

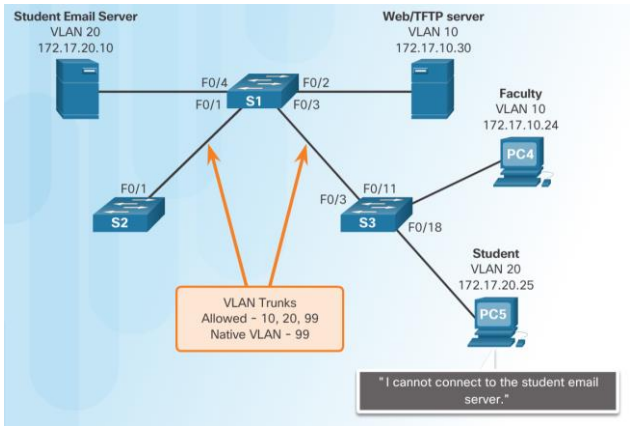
Check the status of the trunk ports on switch S1 using the **show interfaces trunk** command. The output shown in Figure 2 reveals that interface Fa0/3 on switch S1 is not currently a trunk link. Examining the F0/3 interface reveals that the switch port is configured statically in trunk mode. An examination of the trunks on switch S3 reveals that there are no active trunk ports. Further checking reveals that the Fa0/3 interface is in static access mode. This is because the port was configured using the **switchport mode access** command. This explains why the trunk is down.

To resolve the issue, reconfigure the trunk mode of the F0/3 ports on switch S3, as shown in Figure 3. After the configuration change, the output of the **show interfaces** command indicates that the port on switch S3 is now in trunking. The output from PC4 indicates that it has regained connectivity to the Web/TFTP server found at IPv4 address 172.17.10.30.

Troubleshoot VLANs and Trunks

Incorrect VLAN List

- In this example, PC5 cannot reach the Student Email server.
  - The output of the **switchport trunk allowed vlan** command reveals S1 is not allowing VLAN 20.




```
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
…
S1#
```

To resolve the issue, the S1 F0/1 port is configured to allow VLANs 10, 20, and 99.

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

Incorrect VLAN List

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

In Figure 1, VLAN 20 (Student) and PC5 have been added to the network. The documentation has been updated to show that the VLANs allowed on the trunk are 10, 20, and 99. In this scenario, PC5 cannot connect to the student email server.

Check the trunk ports on switch S1 using the **show interfaces trunk** command as shown in Figure 2. The **show interfaces trunk** command is an excellent tool for revealing common trunking problems. The command reveals that the interface F0/3 on switch S3 is correctly configured to allow VLANs 10, 20, and 99. An examination of the F0/3 interface on switch S1 reveals that interfaces F0/1 and F0/3 only allow VLANs 10 and 99. Someone updated the documentation but forgot to reconfigure the ports on the S1 switch.

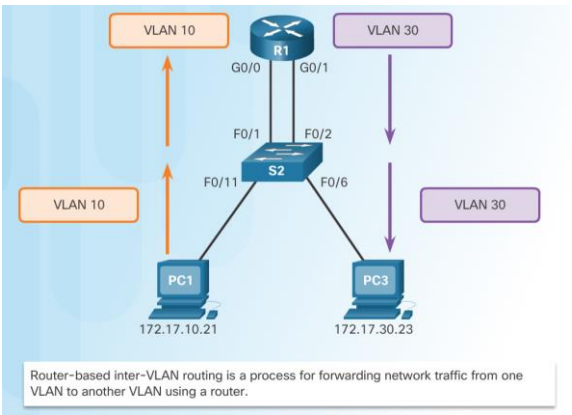
Reconfigure F0/1 and F0/3 on switch S1 using the **switchport trunk allowed vlan 10,20,99** command as shown in Figure 3. The output shows that VLANs 10, 20, and 99 are now added to the F0/1 and F0/3 ports on switch S1. PC5 has regained connectivity to the student email server found at IPv4 address 172.17.20.10.

Inter-VLAN Routing Using Routers

Inter-VLAN Routing Operation

What is Inter-VLAN Routing?

- Layer 2 switches cannot forward traffic between VLANs without the assistance of a router.
- Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a router.
- There are three options for inter-VLAN routing:
  - Legacy inter-VLAN routing
  - Router-on-a-Stick
  - Layer 3 switching using SVI



Router-based inter-VLAN routing is a process for forwarding network traffic from one VLAN to another VLAN using a router.

What is Inter-VLAN Routing?

VLANs are used to segment switched networks. Layer 2 switches, such as the Catalyst 2960 Series, can be configured with over 4,000 VLANs. A VLAN is a broadcast domain, so computers on separate VLANs are unable to communicate without the intervention of a routing device. Layer 2 switches have very limited IPv4 and IPv6 functionality and cannot perform the dynamic routing function of routers. While Layer 2 switches are gaining more IP functionality, such as the ability to perform static routing, this is insufficient to handle these large number of VLANs.

Any device that supports Layer 3 routing, such as a router or a multilayer switch, can be used to perform the necessary routing functionality. Regardless of the device used, the process of forwarding network traffic from one VLAN to another VLAN using routing is known as inter-VLAN routing.

There are three options for inter-VLAN routing:

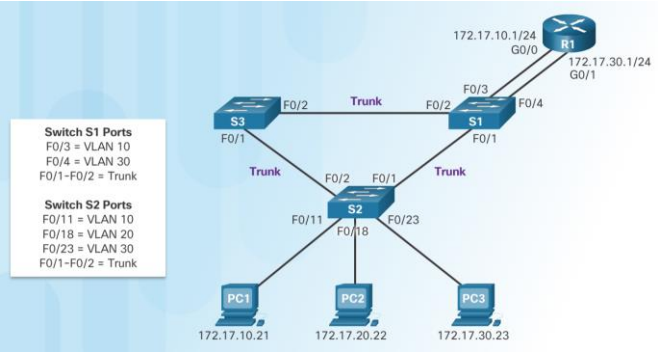
- Legacy inter-VLAN routing
- Router-on-a-Stick
- Layer 3 switching using SVIs

Note: This chapter focuses on the first two options. Layer 3 switching using SVIs is beyond the scope of this course.

Inter-VLAN Routing Operation

Legacy Inter-VLAN Routing

- In the past:
  - Router interfaces were used to route between VLAN.
  - Each VLAN was connected to a different physical router interface.
  - Packets would arrive on the router through one interface, be routed and leave through another.
  - Because the router interfaces were connected to VLAN and had IP addresses from that specific VLAN, routing between VLANs was achieved.
  - Large networks with large number of VLAN required many router interfaces.



In this example, the router was configured with two separate physical interfaces to interact with the different VLAN and perform the routing.

Legacy Inter-VLAN Routing

Historically, the first solution for inter-VLAN routing relied on routers with multiple physical interfaces. Each interface had to be connected to a separate network and configured with a distinct subnet.

In this legacy approach, inter-VLAN routing is performed by connecting different physical router interfaces to different physical switch ports. The switch ports connected to the router are placed in access mode and each physical interface is assigned to a different VLAN. Each router interface can then accept traffic from the VLAN associated with the switch interface that it is connected to, and traffic can be routed to the other VLANs connected to the other interfaces.

Follows an example of legacy inter-VLAN routing:

1. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through router R1.
2. PC1 and PC3 are on different VLAN and have IPv4 addresses on different subnets.
3. Router R1 has a separate interface configured for each of the VLAN.
4. PC1 sends unicast traffic destined for PC3 to switch S2 on VLAN 10, where it is then forwarded out the trunk interface to switch S1.
5. Switch S1 then forwards the unicast traffic through its interface F0/3 to interface G0/0 on router R1.
6. The router routes the unicast traffic through its interface G0/1, which is connected to VLAN 30.
7. The router forwards the unicast traffic to switch S1 on VLAN 30.
8. Switch S1 then forwards the unicast traffic to switch S2 through the active trunk

link, after which switch S2 can then forward the unicast traffic to PC3 on VLAN 30. In this example, the router was configured with two separate physical interfaces to interact with the different VLANs and perform the routing.

Note: This method of inter-VLAN routing is not efficient and is generally no longer implemented in switched networks. It is shown in this course for explanation purposes only.

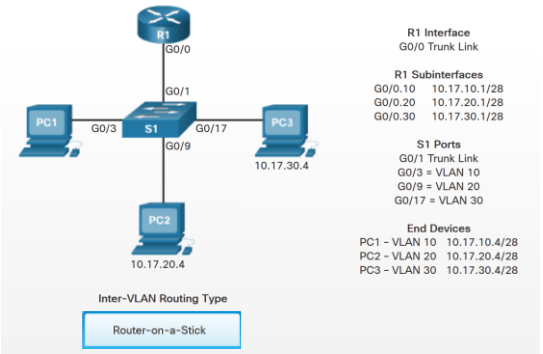
Activity – Identify the types of inter-VLAN routing (1)

Identify this topology as a legacy, router-on-a-stick, or multilayer switch inter-VLAN routing by dragging the appropriate answer to the field provided.

Multilayer Switch

Router-on-a-Stick

Legacy



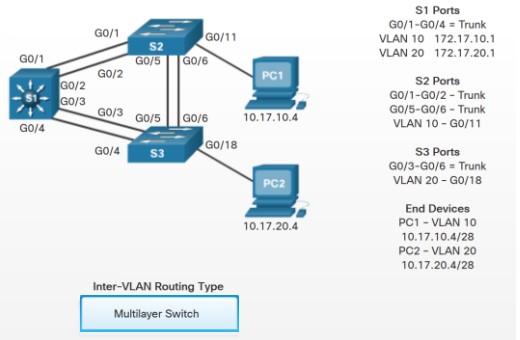
Activity – Identify the types of inter-VLAN routing (2)

Identify this topology as a legacy, router-on-a-stick, or multilayer switch inter-VLAN routing by dragging the appropriate answer to the field provided.

Multilayer Switch

Router-on-a-Stick

Legacy



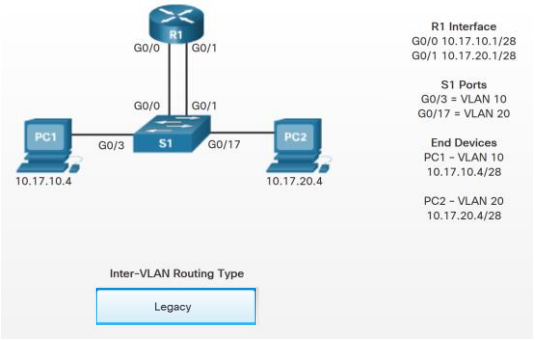
Activity – Identify the types of inter-VLAN routing (3)

Identify this topology as a legacy, router-on-a-stick, or multilayer switch inter-VLAN routing by dragging the appropriate answer to the field provided.

Multilayer Switch

Router-on-a-Stick

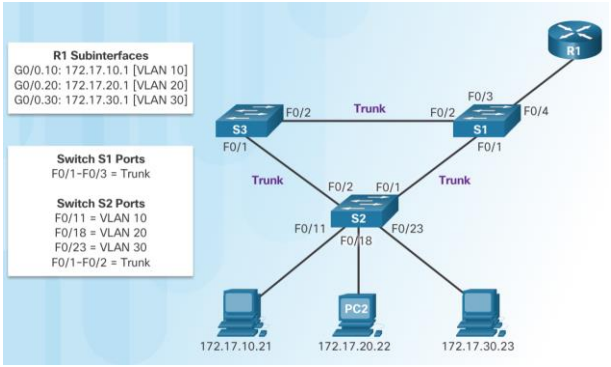
Legacy



Inter-VLAN Routing Operation

Router-on-a-Stick Inter-VLAN Routing

- The router-on-a-stick approach uses only one of the router's physical interface.
  - One of the router's physical interfaces is configured as an 802.1Q trunk port so it can understand VLAN tags.
  - Logical subinterfaces are created; one subinterface per VLAN.
  - Each subinterface is configured with an IP address from the VLAN it represents.
  - VLAN members (hosts) are configured to use the subinterface address as a default gateway.



In this example, the R1 interface is configured as a trunk link and connects to the trunk F0/4 port on S1.

- Router accepts VLAN-tagged traffic on the trunk interface
- Router internally routes between the VLAN using subinterfaces.
- Router then forwards the routed traffic as VLAN-tagged for the destination VLAN out the trunk link.

Router-on-a-Stick Inter-VLAN Routing

While legacy inter-VLAN routing requires multiple physical interfaces on both the router and the switch, a more common, present-day implementation of inter-VLAN routing does not. Instead, some router software permits configuring a router interface as a trunk link, meaning only one physical interface is required on the router and the switch to route packets between multiple VLANs.

'Router-on-a-stick' is a type of router configuration in which a single physical interface routes traffic between multiple VLANs on a network. As seen in the figure, the router is connected to switch S1 using a single, physical network connection (a trunk).

The router interface is configured to operate as a trunk link and is connected to a switch port that is configured in trunk mode. The router performs inter-VLAN routing by accepting VLAN-tagged traffic on the trunk interface coming from the adjacent switch, and then, internally routing between the VLANs using subinterfaces. The router then forwards the routed traffic, VLAN-tagged for the destination VLAN, out the same physical interface as it used to receive the traffic.

Subinterfaces are software-based virtual interfaces, associated with a single physical interface. Subinterfaces are configured in software on a router and each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets corresponding to their VLAN assignment to facilitate logical routing. After a routing decision is made based on the destination VLAN, the data frames are VLAN-tagged and sent back out the physical interface.

Follows an example how a router-on-a-stick performs its routing function:

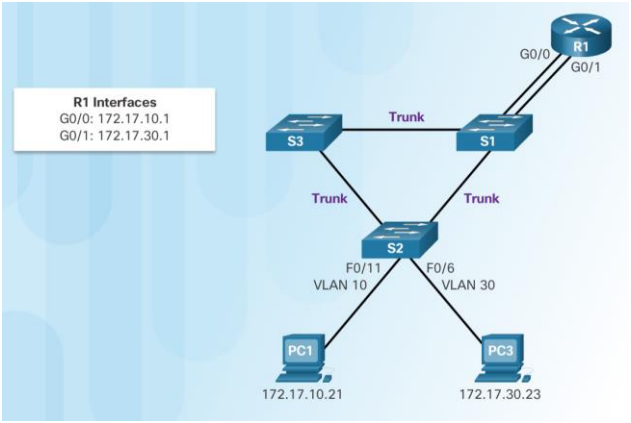
1. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through router R1 using a single, physical router interface.
2. PC1 sends its unicast traffic to switch S2.
3. Switch S2 then tags the unicast traffic as originating on VLAN 10 and forwards the unicast traffic out its trunk link to switch S1.
4. Switch S1 forwards the tagged traffic out the other trunk interface on port F0/3 to the interface on router R1.
5. Router R1 accepts the tagged unicast traffic on VLAN 10 and routes it to VLAN 30 using its configured subinterfaces.
6. The unicast traffic is tagged with VLAN 30 as it is sent out the router interface to switch S1.
7. Switch S1 forwards the tagged unicast traffic out the other trunk link to switch S2.
8. Switch S2 removes the VLAN tag of the unicast frame and forwards the frame out to PC3 on port F0/23.

Note: The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.

Configure Legacy Inter-VLAN Routing

Configure Legacy Inter-VLAN Routing: Preparation

- Legacy inter-VLAN routing requires routers to have multiple physical interfaces.
- Each one of the router's physical interfaces is connected to a unique VLAN.
- Each interface is also configured with an IP address for the subnet associated with the particular VLAN.
- Network devices use the router as a gateway to access the devices connected to the other VLANs.



Configure Legacy Inter-VLAN Routing: Preparation

Legacy inter-VLAN routing requires routers to have multiple physical interfaces. The router accomplishes the routing by having each of its physical interfaces connected to a unique VLAN. Each interface is also configured with an IPv4 address for the subnet associated with the particular VLAN to which it is connected. By configuring the IPv4 addresses on the physical interfaces, network devices connected to each of the VLANs can communicate with the router using the physical interface connected to the same VLAN. In this configuration, network devices can use the router as a gateway to access the devices connected to the other VLANs.

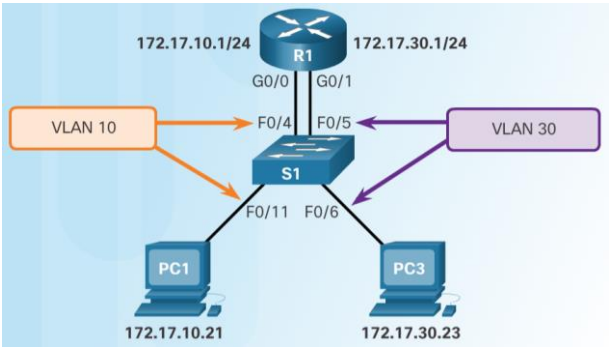
The routing process requires the source device to determine if the destination device is local or remote to the local subnet. The source device accomplishes this by comparing the source and destination IPv4 addresses against the subnet mask. When the destination IPv4 address has been determined to be on a remote network, the source device must identify where it needs to forward the packet to reach the destination device. The source device examines the local routing table to determine where it needs to send the data. Devices use their default gateway as the Layer 2 destination for all traffic that must leave the local subnet. The default gateway is the route that the device uses when it has no other explicitly defined route to the destination network. The IPv4 address of the router interface on the local subnet acts as the default gateway for the sending device.

When the source device has determined that the packet must travel through the local router interface on the connected VLAN, the source device sends out an ARP request

to determine the MAC address of the local router interface. When the router sends its ARP reply back to the source device, the source device can use the MAC address to finish framing the packet before it sends it out on the network as unicast traffic. Because the Ethernet frame has the destination MAC address of the router interface, the switch knows exactly which switch port to forward the unicast traffic out of to reach the router interface for that VLAN. When the frame arrives at the router, the router removes the source and destination MAC address information to examine the destination IPv4 address of the packet. The router compares the destination address to entries in its routing table to determine where it needs to forward the data to reach its final destination. If the router determines that the destination network is a locally connected network, as is the case with inter-VLAN routing, the router sends an ARP request out the interface that is physically connected to the destination VLAN. The destination device responds back to the router with its MAC address, which the router then uses to frame the packet. The router then sends the unicast traffic to the switch, which forwards it out the port where the destination device is connected. Even though there are many steps in the process of inter-VLAN routing, when two devices on different VLANs communicate through a router, the entire process happens in a fraction of a second.

Configure Legacy Inter-VLAN Routing

Configure Legacy Inter-VLAN Routing: Switch Configuration



- Configure the VLAN on the switch and then assign the ports to their respective VLAN.
- In this example, the S1 ports are configured as follows:
  - Ports F0/4 and F0/11 of S1 are on VLAN 10
  - Ports F0/5 and F0/16 ports are on VLAN 30.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
```


Configure Legacy Inter-VLAN Routing: Switch Configuration

To configure legacy inter-VLAN routing, start by configuring the switch.

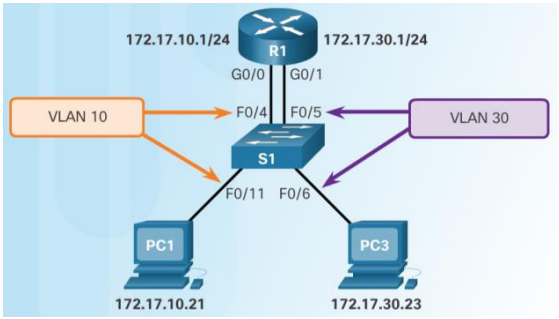
As shown in the figure, router R1 is connected to switch ports F0/4 and F0/5, which have been configured for VLANs 10 and 30, respectively.

Use the **vlan** *vlan_id* global configuration mode command to create VLANs. In this example, VLANs 10 and 30 were created on switch S1.

After the VLANs have been created, the switch ports are assigned to the appropriate VLANs. The **switchport access vlan** *vlan_id* command is executed from interface configuration mode on the switch for each interface to which the router connects. In this example, interfaces F0/4 and F0/11 have been assigned to VLAN 10 using the **switchport access vlan 10** command. The same process is used to assign interface F0/5 and F0/6 on switch S1 to VLAN 30.

Finally, to protect the configuration so that it is not lost after a reload of the switch, the **copy running-config startup-config** command is executed to back up the running configuration to the startup configuration.

Configure Legacy Inter-VLAN Routing: Router Interface config



- Next configure the router interfaces.

```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
```


Configure Legacy Inter-VLAN Routing: Router Interface Configuration

Now the router can be configured to perform inter-VLAN routing.

Router interfaces are configured in a manner similar to configuring VLAN interfaces on switches. To configure a specific interface, change to interface configuration mode from global configuration mode.

As shown in Figure, each interface is configured with an IPv4 address using the**ip address** *ip_address subnet_mask*command in interface configuration mode.

In the example, interface G0/0 is configured with IPv4 address 172.17.10.1 and subnet mask 255.255.255.0 using the**ip address 172.17.10.1 255.255.255.0** command.

Router interfaces are disabled by default and must be enabled using the**no shutdown**command before they are used. After the**no shutdown**interface configuration mode command has been issued, a notification displays, indicating that the interface state has changed to up. This indicates that the interface is now enabled.

The process is repeated for all router interfaces. Each router interface must be assigned to a unique subnet for routing to occur. In this example, the other router interface, G0/1, has been configured to use IPv4 address 172.17.30.1, which is on a different subnet than interface G0/0.

After the IPv4 addresses are assigned to the physical interfaces and the interfaces are enabled, the router is capable of performing inter-VLAN routing.

Examine the routing table using the **show ip route**command.

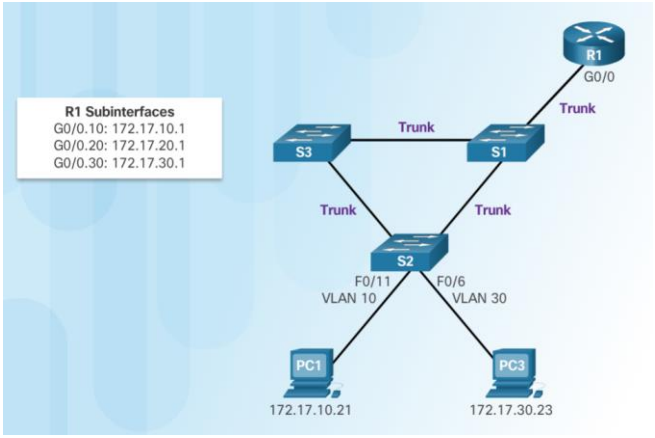
There are two routes visible in the routing table. One route is to the 172.17.10.0 subnet, which is attached to the local interface G0/0. The other route is to the 172.17.30.0 subnet, which is attached to the local interface G0/1. The router uses this routing table to determine where to send the traffic it receives. For example, if the router receives a packet on interface G0/0 destined for the 172.17.30.0 subnet, the router would identify that it should send the packet out interface G0/1 to reach hosts on the 172.17.30.0 subnet.

Notice the letter **C** to the left of each of the route entries for the VLANs. This letter indicates that the route is local for a connected interface, which is also identified in the route entry.

Configure Router-on-a-Stick Inter-VLAN Routing

Configure Router-on-a Stick: Preparation

- An alternative to legacy inter-VLAN routing is to use VLAN trunking and subinterfaces.
- VLAN trunking allows a single physical router interface to route traffic for multiple VLAN.
- The physical interface of the router must be connected to a trunk link on the adjacent switch.
- On the router, subinterfaces are created for each unique VLAN.
- Each subinterface is assigned an IP address specific to its subnet or VLAN and is also configured to tag frames for that VLAN.



Configure Router-on-a-Stick: Preparation

Legacy inter-VLAN routing using physical interfaces has a significant limitation. Routers have a limited number of physical interfaces to connect to different VLANs. As the number of VLANs increases on a network, having one physical router interface per VLAN quickly exhausts the physical interface capacity of a router. An alternative in larger networks is to use VLAN trunking and subinterfaces. VLAN trunking allows a single physical router interface to route traffic for multiple VLANs. This technique is termed router-on-a-stick and uses virtual subinterfaces on the router to overcome the hardware limitations based on physical router interfaces.

Subinterfaces are software-based virtual interfaces that are assigned to physical interfaces. Each subinterface is configured independently with its own IP address and prefix length. This allows a single physical interface to simultaneously be part of multiple logical networks.

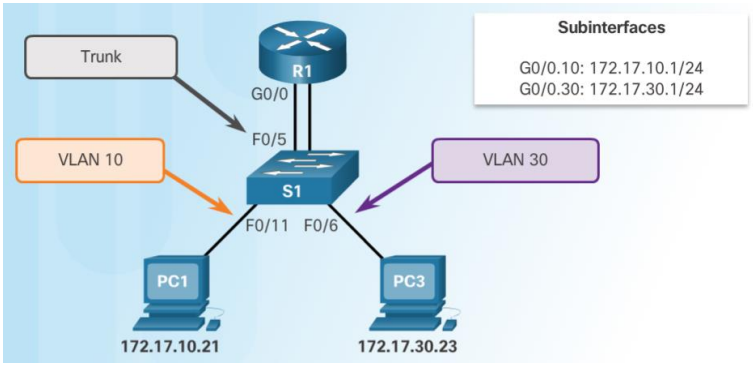
Note: The term prefix length can be used to refer to the IPv4 subnet mask when associated with an IPv4 address, and the IPv6 prefix length when associated with an IPv6 address.

When configuring inter-VLAN routing using the router-on-a-stick model, the physical interface of the router must be connected to a trunk link on the adjacent switch. On the router, subinterfaces are created for each unique VLAN on the network. Each subinterface is assigned an IP address specific to its subnet/VLAN and is also configured to tag frames for that VLAN. This way, the router can keep the traffic from each subinterface separate as it traverses the trunk link back to the switch.

Functionally, the router-on-a-stick model is the same as using the legacy inter-VLAN routing model, but instead of using the physical interfaces to perform the routing, subinterfaces of a single physical interface are used.
In the figure, PC1 wants to communicate with PC3. PC1 is on VLAN 10 and PC3 is on VLAN 30. For PC1 to communicate with PC3, PC1 must have its data routed through router R1 via subinterfaces.
Using trunk links and subinterfaces decreases the number of router and switch ports used. Not only can this save money, it can also reduce configuration complexity. Consequently, the router subinterface approach can scale to a much larger number of VLANs than a configuration with one physical interface per VLAN design.

Configure Router-on-a-Stick Inter-VLAN Routing

Configure Router-on-a Stick: Switch Configuration



- To enable inter-VLAN routing using router-on-a stick, start by enabling trunking on the switch port that is connected to the router.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```


Configure Router-on-a-Stick: Switch Configuration

To enable inter-VLAN routing using router-on-a stick, start by enabling trunking on the switch port that is connected to the router.

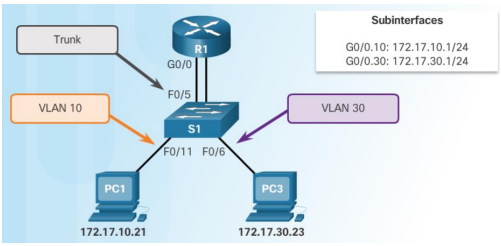
In the figure, router R1 is connected to switch S1 on trunk port F0/5. VLANs 10 and 30 are added to switch S1.

Because switch port F0/5 is configured as a trunk port, the port does not need to be assigned to any VLAN. To configure switch port F0/5 as a trunk port, execute the **switchport mode trunk** command in interface configuration mode for port F0/5.

The router can now be configured to perform inter-VLAN routing.

Configure Router-on-a-Stick Inter-VLAN Routing

Configure Router-on-a Stick: Router Subinterface Configuration



- The router-on-a-stick method requires subinterfaces to be configured for each routable VLAN.
  - The subinterfaces must be configured to support VLANs using the **encapsulation dot1Q** *VLAN-ID* interface configuration command.

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface   GigabitEthernet0/0, changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```


Configure Router-on-a-Stick: Router Subinterface Configuration

The configuration of the router is different when a router-on-a-stick configuration is used, compared to legacy inter-VLAN routing. The figure shows that multiple subinterfaces are configured.

Each subinterface is created using the **interface** *interface_id subinterface_id* global configuration mode command. The syntax for the subinterface is the physical interface, in this case g0/0, followed by a period and a subinterface number. As shown in the figure subinterface GigabitEthernet0/0.10 is created using the **interface g0/0.10 global** configuration mode command. The subinterface number is typically configured to reflect the VLAN number.

Before assigning an IP address to a subinterface, the subinterface must be configured to operate on a specific VLAN using the **encapsulation dot1q** *vlan_id* command. In this example, subinterface G0/0.10 is assigned to VLAN 10.

Note: There is a **native** keyword option that can be appended to this command to set the IEEE 802.1Q native VLAN. In this example, the **native** keyword option was excluded to leave the native VLAN default as VLAN 1.

Next, assign the IPv4 address for the subinterface using the **ip address** *ip_address subnet_mask* subinterface configuration mode command. In this example, subinterface G0/0.10 is assigned the IPv4 address 172.17.10.1 using the **ip address 172.17.10.1 255.255.255.0** command.

This process is repeated for all router subinterfaces required to route between the VLANs configured on the network. Each router subinterface must be assigned an IP

address on a unique subnet for routing to occur. For example, the other router subinterface, G0/0.30, is configured to use IPv4 address 172.17.30.1, which is on a different subnet from subinterface G0/0.10.

After a physical interface is enabled, subinterfaces will automatically be enabled upon configuration. Subinterfaces do not need to be enabled with the **no shutdown** command at the subinterface configuration mode level of the Cisco IOS software.

If the physical interface is disabled, all subinterfaces are disabled. In this example, the command **no shutdown** is entered in interface configuration mode for interface G0/0, which in turn, enables all of the configured subinterfaces.

Individual subinterfaces can be administratively shut down with the **shutdown** command. Also, individual subinterfaces can be enabled independently with the **no shutdown** command in the subinterface configuration mode.

Configure Router-on-a-Stick Inter-VLAN Routing

Configure Router-on-a Stick: Verifying Subinterfaces

- By default, Cisco routers are configured to route traffic between local subinterfaces.
  - As a result, routing does not specifically need to be enabled.
- Use the **show vlan** and **show ip route** commands to verify the subinterface configurations.

```
R1# show vlan
<output omitted>

Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.10

  Protocols Configured:     Address:          Received:       Transmitted:
         IP                 172.17.10.1            11                18
<output omitted>

Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.30

  Protocols Configured:     Address:          Received:       Transmitted:
         IP                 172.17.30.1            11                8
<output omitted>
```

The **show vlan** command displays information about the Cisco IOS VLAN subinterfaces.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF, IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, i - IS-IS,
       su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP,
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C     172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L     172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C     172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L     172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

The **show ip route** command displays the routing table containing the networks associated with outgoing subinterfaces.

Configure Router-on-a-Stick: Verifying Subinterfaces

By default, Cisco routers are configured to route traffic between local subinterfaces. As a result, routing does not specifically need to be enabled.

In Figure 1, the **show vlan** command displays information about the Cisco IOS VLAN subinterfaces. The output shows the two VLAN subinterfaces, GigabitEthernet0/0.10 and GigabitEthernet0/0.30.

Examine the routing table using the **show ip route** command (Figure 2). In the example, the routes defined in the routing table indicate that they are associated with specific subinterfaces, rather than separate physical interfaces. There are two routes in the routing table. One route is to the 172.17.10.0 subnet, which is attached to the local subinterface G0/0.10. The other route is to the 172.17.30.0 subnet, which is attached to the local subinterface G0/0.30. The router uses this routing table to determine where to send the traffic it receives. For example, if the router received a packet on subinterface G0/0.10 destined for the 172.17.30.0 subnet, the router would identify that it should send the packet out subinterface G0/0.30 to reach hosts on the 172.17.30.0 subnet.

Configure Router-on-a-Stick Inter-VLAN Routing

Configure Router-on-a Stick: Verifying Routing

- Remote VLAN device connectivity can be tested using the **ping** command.
  - The command sends an ICMP echo request and when a host receives an ICMP echo request, it responds with an ICMP echo reply.

```
PC1> ping 172.17.30.23

Pinging 172.17.30.23 with 32 bytes of data:

Reply from 172.17.30.23: bytes=32 time=17ms TTL=127
Reply from 172.17.30.23: bytes=32 time=15ms TTL=127
Reply from 172.17.30.23: bytes=32 time=18ms TTL=127
Reply from 172.17.30.23: bytes=32 time=19ms TTL=127

Ping statistics for 172.17.30.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

- **Tracert** is a useful utility for confirming the routed path taken between two devices.

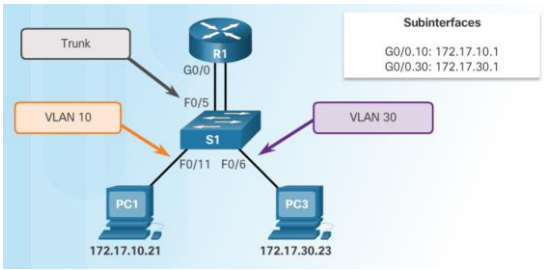
```
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 19ms, Average = 17ms

PC1> tracert 172.17.30.23

Tracing route to 172.17.30.23 over a maximum of 30 hops:

 1    9 ms      7 ms      9 ms      172.17.10.1
 2   16 ms     15 ms     16 ms      172.17.30.23

Trace complete.
```



Configure Router-on-a-Stick: Verifying Routing

After the router and switch have been configured to perform inter-VLAN routing, the next step is to verify host-to-host connectivity. Access to devices on remote VLAN can be tested using the **ping** command.

For the example shown in the figure, a **ping** and a **tracert** are initiated from PC1 to the destination address of PC3.

Ping Test

The **ping** command sends an ICMP echo request to the destination address. When a host receives an ICMP echo request, it responds with an ICMP echo reply to confirm that it received the ICMP echo request. The **ping** command calculates the elapsed time using the difference between the time the echo request was sent and the time the echo reply was received. This elapsed time is used to determine the latency of the connection. Successfully receiving a reply confirms that there is a path between the sending device and the receiving device.

Tracert Test

Tracert is a useful utility for confirming the routed path taken between two devices. On UNIX systems, the utility is specified by **traceroute.** Tracert also uses ICMP to determine the path taken, but it uses ICMP echo requests with specific time-to-live values defined on the frame.

The time-to-live value determines exactly how many router hops away the ICMP echo

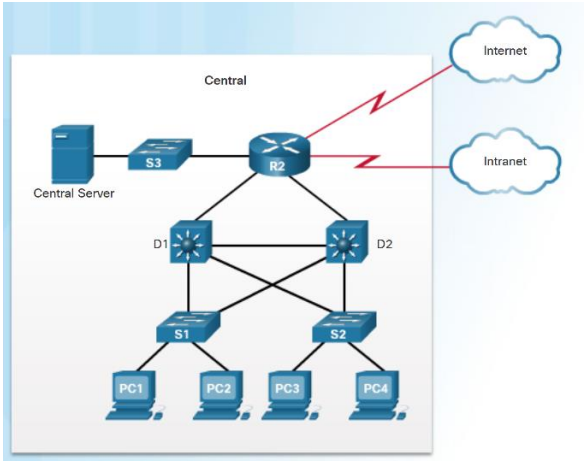
is allowed to reach. The first ICMP echo request is sent with a time-to-live value set to expire at the first router on route to the destination device.
When the ICMP echo request times out on the first route, an ICMP message is sent back from the router to the originating device. The device records the response from the router and proceeds to send out another ICMP echo request, but this time with a greater time-to-live value. This allows the ICMP echo request to traverse the first router and reach the second device on route to the final destination. The process repeats recursively until finally the ICMP echo request is sent all the way to the final destination device. After the **tracert** utility finishes running, it displays a list of ingress router interfaces that the ICMP echo request reached on its way to the destination.
In the example, the **ping** utility was able to send an ICMP echo request to the IP address of PC3. Also, the **tracert** utility confirms that the path to PC3 is through the 172.17.10.1 subinterface IP address of router R1.

Layer 3 Switching

2 – Scaling VLANs
2.3 – Layer 3 Switching

Layer 3 Switching Operation and Configuration

Introduction to Layer 3 Switching



- Multilayer switches provide high-packet processing rates using hardware-based switching.
- Catalyst multilayer switches support the following types of Layer 3 interfaces:
  - **Routed port** - A layer 3 interface
  - **Switch virtual interface (SVI)** - Virtual Interface for inter- VLAN routing
- All Layer 3 Cisco Catalyst switches support routing protocols, but several models require enhanced software for specific routing protocol features.
- Catalyst 2960 Series switches running IOS 12.2(55) or later, support static routing.

Introduction to Layer 3 Switching

Inter-VLAN routing using the router-on-a-stick method was simple to implement because routers were usually available in every network. However, as shown in the figure, most modern enterprise networks use multilayer switches to achieve high-packet processing rates using hardware-based switching. Layer 3 switches usually have packet-switching throughputs in the millions of packets per second (pps), whereas traditional routers provide packet switching in the range of 100,000 pps to more than 1 million pps.

All Catalyst multilayer switches support the following types of Layer 3 interfaces:

Routed port - A pure Layer 3 interface similar to a physical interface on a Cisco IOS router.

Switch virtual interface (SVI) - A virtual VLAN interface for inter-VLAN routing. In other words, SVIs are the virtual-routed VLAN interfaces.

High-performance switches, such as the Catalyst 6500 and Catalyst 4500, perform almost every function involving OSI Layer 3 and higher using hardware-based switching that is based on Cisco Express Forwarding.

All Layer 3 Cisco Catalyst switches support routing protocols, but several models of Catalyst switches require enhanced software for specific routing protocol features. Catalyst 2960 Series switches running IOS Release 12.2(55) or later, support static routing.

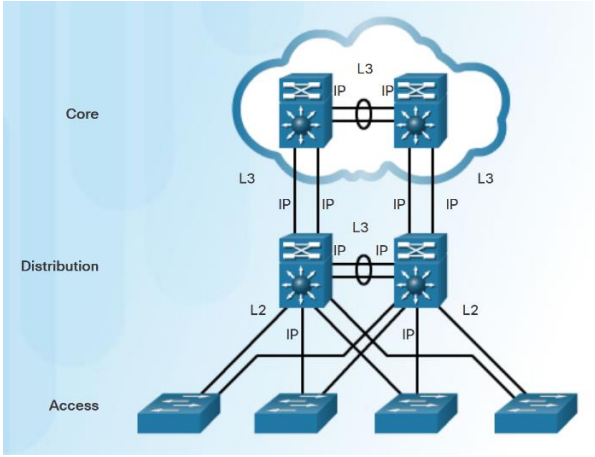
Catalyst switches use different default settings for interfaces. All members of the Catalyst 3560 and 4500 families of switches use Layer 2 interfaces by default.

Members of the Catalyst 6500 family of switches running Cisco IOS use Layer 3 interfaces by default. Depending on which Catalyst family of switches is used, the **switchport** or **no switchport** interface configuration mode commands might be present in the running config or startup configuration files.

Layer 3 Switching Operation and Configuration

Inter-VLAN Routing with Switch Virtual Interfaces

- In the early days of switched networks, switching was fast and routing was slow. Therefore the layer 2 switching portion was extended as much as possible into the network.
- Now routing can be performed at wire speed, and is performed at both the distribution and core layers.
- Distribution switches are configured as Layer 3 gateways using Switch Virtual Interfaces (SVIs) or routed ports.
- Routed ports are usually implemented between the distribution and core layers.



nter-VLAN Routing with Switch Virtual Interfaces

In the early days of switched networks, switching was fast (often at hardware speed, meaning the speed was equivalent to the time it took to physically receive and forward frames onto other ports) and routing was slow (routing had to be processed in software). This prompted network designers to extend the switched portion of the network as much as possible. Access, distribution, and core layers were often configured to communicate at Layer 2. This topology created loop issues. To solve these issues, spanning-tree technologies were used to prevent loops while still enabling flexibility and redundancy in inter-switch connections.

However, as network technologies have evolved, routing has become faster and cheaper. Today, routing can be performed at wire speed. One consequence of this evolution is that routing can be transferred to the core and the distribution layers (and sometimes even the access layer) without impacting network performance.

Many users are in separate VLANs, and each VLAN is usually a separate subnet. Therefore, it is logical to configure the distribution switches as Layer 3 gateways for the users of each access switch VLAN. This implies that each distribution switch must have IP addresses matching each access switch VLAN. This can be achieved by using Switch Virtual Interfaces (SVIs) and routed ports.

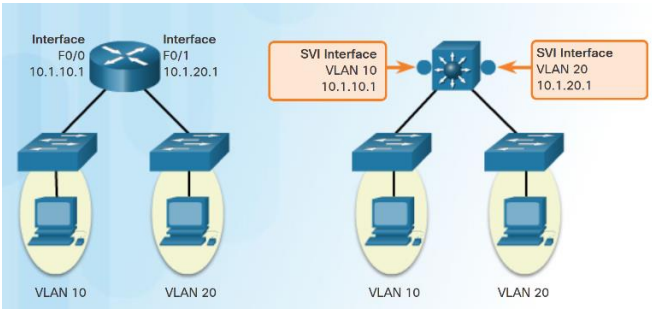
Layer 3 (routed) ports are normally implemented between the distribution and the core layer.

The network architecture depicted is not dependent on spanning tree because there are no physical loops in the Layer 2 portion of the topology.

Layer 3 Switching Operation and Configuration

Inter-VLAN Routing with Switch Virtual Interfaces (Cont.)

- An SVI is a virtual interface that is configured within a multilayer switch:
  - To provide a gateway for a VLAN so that traffic can be routed into or out of that VLAN.
  - To provide Layer 3 IP connectivity to the switch.
  - To support routing protocol and bridging configurations.
- Advantages of SVIs:
  - Faster than router-on-a-stick.
  - No need for external links from the switch to the router for routing.
  - Not limited to one link. Layer 2 EtherChannels can be used to get more bandwidth.



Inter-VLAN Routing with Switch Virtual Interfaces (Cont.)

An SVI is a virtual interface that is configured within a multilayer switch, as shown in the figure. An SVI can be created for any VLAN that exists on the switch. An SVI is considered to be virtual because there is no physical port dedicated to the interface. It can perform the same functions for the VLAN as a router interface would, and can be configured in much the same way as a router interface (i.e., IP address, inbound/outbound ACLs, etc.). The SVI for the VLAN provides Layer 3 processing for packets to or from all switch ports associated with that VLAN.

By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly created. SVIs are created the first time the VLAN interface configuration mode is entered for a particular VLAN SVI, such as when the **interface vlan 10** command is entered. The VLAN number used corresponds to the VLAN tag associated with data frames on an 802.1Q encapsulated trunk or to the VLAN ID (VID) configured for an access port. When creating an SVI as a gateway for VLAN 10, name the SVI interface VLAN 10. Configure and assign an IP address to each VLAN SVI.

Whenever the SVI is created, ensure that particular VLAN is present in the VLAN database. In the figure, the switch should have VLAN 10 and VLAN 20 present in the VLAN database; otherwise, the SVI interface stays down.

The following are some of the reasons to configure SVI:

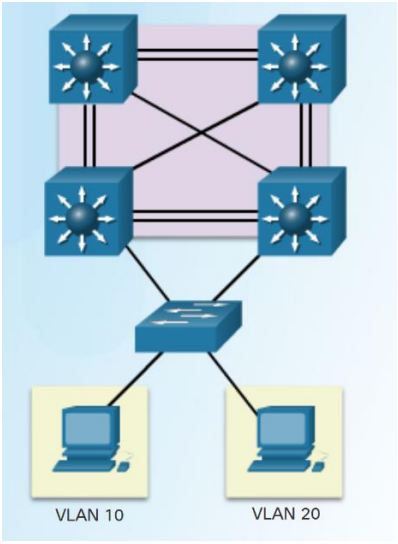
To provide a gateway for a VLAN so that traffic can be routed into or out of that VLAN

To provide Layer 3 IP connectivity to the switch

To support routing protocol and bridging configurations
The following are some of the advantages of SVIs (the only disadvantage is that multilayer switches are more expensive):
It is much faster than router-on-a-stick, because everything is hardware switched and routed.
No need for external links from the switch to the router for routing.
Not limited to one link. Layer 2 EtherChannels can be used between the switches to get more bandwidth.
Latency is much lower, because data does not need to leave the switch in order to be routed to a different network.

Layer 3 Switching Operation and Configuration

Inter-VLAN Routing with Routed Ports



- A routed port is a physical port that acts similarly to an interface on a router:
  - It is not associated with a particular VLAN.
  - It does not support subinterfaces.
- Routed ports are primarily configured between switches in the core and distribution layer.
- Use the **no switchport interface** command on the appropriate port to configure a routed port.

Note: Routed ports are not supported on Catalyst 2960 Series switches.

Inter-VLAN Routing with Routed Ports

Routed Ports and Access Ports on a Switch

A routed port is a physical port that acts similarly to an interface on a router. Unlike an access port, a routed port is not associated with a particular VLAN. A routed port behaves like a regular router interface. Also, because Layer 2 functionality has been removed, Layer 2 protocols, such as STP, do not function on a routed interface. However, some protocols, such as LACP and EtherChannel, do function at Layer 3. Unlike Cisco IOS routers, routed ports on a Cisco IOS switch do not support subinterfaces.

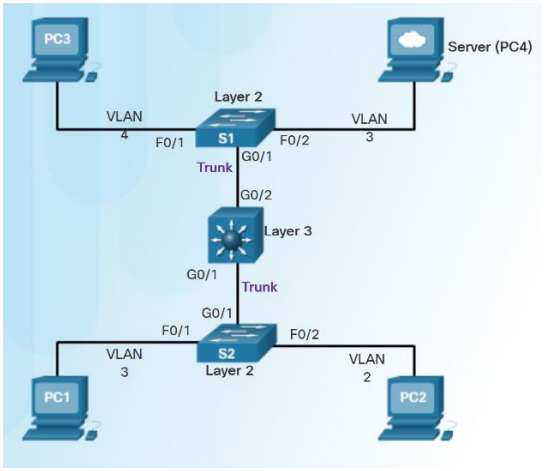
Routed ports are used for point-to-point links. Connecting WAN routers and security devices are examples of the use of routed ports. In a switched network, routed ports are mostly configured between switches in the core and distribution layer. The figure illustrates an example of routed ports in a campus switched network.

To configure routed ports, use the **no switchport** interface configuration mode command on the appropriate ports. For example, the default configuration of the interfaces on Catalyst 3560 switches are Layer 2 interfaces, so they must be manually configured as routed ports. In addition, assign an IP address and other Layer 3 parameters as necessary. After assigning the IP address, verify that IP routing is globally enabled and that applicable routing protocols are configured.

Note: Routed ports are not supported on Catalyst 2960 Series switches.

Troubleshoot Layer 3 Switching

Layer 3 Switch Configuration Issues



- To troubleshoot Layer 3 switching issues check the following:
  - **VLANs** – verify correct configuration.
  - **SVIs** - verify correct IP, subnet mask and VLAN number.
  - **Routing** - verify that either static or dynamic routing is correctly configured and enabled.
  - **Hosts** – verify correct IP, subnet mask, and default gateway.

Layer 3 Switch Configuration Issues

The issues common to legacy inter-VLAN routing and router-on-a-stick inter-VLAN routing are also manifested in the context of Layer 3 switching. To troubleshoot Layer 3 switching issues, the following items should be checked for accuracy:

VLANs - VLANs must be defined across all the switches. VLANs must be enabled on the trunk ports. Ports must be in the right VLANs.

SVIs - SVIs must have the correct IP address or subnet mask. SVIs must be up. Each SVI must match with the VLAN number.

Routing - Routing must be enabled. Each interface or network should be added to the routing protocol or static routes entered, where appropriate.

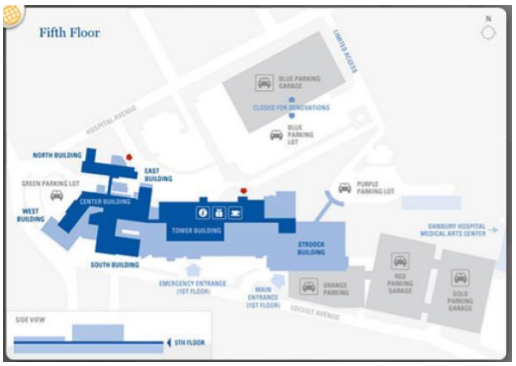
Hosts - Hosts must have the correct IP address or subnet mask. Hosts must have a default gateway associated with an SVI or routed port.

To troubleshoot the Layer 3 switching problems, be familiar with the implementation and design layout of the topology.

Troubleshoot Layer 3 Switching

Example: Troubleshooting Layer 3 Switching

- There are four steps to implementing a new VLAN:
  - **Step 1.** Create and name a new VLAN 500 on the fifth floor switch and on the distribution switches.
  - **Step 2.** Add ports to VLAN 500 and ensure that the trunk is set up between distribution switches.
  - **Step 3.** Create an SVI interface on the distribution switches and ensure that IP addresses are assigned.
  - **Step 4.** Verify connectivity.
- The troubleshooting plan checks for the following:
  - **Step 1.** Verify that all VLANs have been created.
  - **Step 2.** Ensure that ports are in the right VLAN and trunking is working as expected.
  - **Step 3.** Verify SVI configurations.



Example: Troubleshooting Layer 3 Switching

Company XYZ is adding a new floor, floor 5, to the network. Based on this, the current requirements are to make sure the users on floor 5 can communicate with users on other floors. Currently, users on floor 5 cannot communicate with users on other floors. The following is an implementation plan to install a new VLAN for users on floor 5 and to ensure the VLAN is routing to other VLANs.

There are four steps to implementing a new VLAN:

Step 1. Create a new VLAN 500 on the fifth floor switch and on the distribution switches. Name this VLAN.

Step 2. Identify the ports needed for the users and switches. Set the **switchport access vlan** command to **500** and ensure that the trunk between the distribution switches is properly configured and that VLAN 500 is allowed on the trunk.

Step 3. Create an SVI interface on the distribution switches and ensure that IP addresses are assigned.

Step 4. Verify connectivity.

The troubleshooting plan checks for the following:

Step 1. Verify that all VLANs have been created:

Was the VLAN created on all the switches?

Verify with the **show vlan** command.

Step 2. Ensure that ports are in the right VLAN and trunking is working as expected:

Did all access ports have the **switchport access VLAN 500** command added?

Were there any other ports that should have been added? If so, make those changes.

Were these ports previously used? If so, ensure that there are no extra commands enabled on these ports that can cause conflicts. If not, is the port enabled?
Are any user ports set to trunks? If so, issue the **switchport mode access** command.
Are the trunk ports set to trunk mode?
Is manual pruning of VLANs configured? If so, ensure that the trunks necessary to carry VLAN 500 traffic have the VLAN in the allowed statements.
Step 3. Verify SVI configurations (if necessary):
Is the SVI already created with the correct IP address and subnet mask?
Is it enabled?
Is routing enabled?

Chapter Summary

6 - VLANs
6.4 – Summary

Conclusion

Chapter 1: Inter-VLAN routing

- Explain how VLANs segment broadcast domains in a small to medium-sized business network.
- Implement VLANs to segment a small to medium-sized business network..
- Configure routing between VLANs in a small to medium-sized business network.
- Implement inter-VLAN routing using Layer 3 switching to forward data in a small to medium-sized business LAN.
- Configure enhanced inter-switch connectivity technologies.
- Troubleshoot issues in an inter-VLAN routing environment.

VLAN

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

There are several types of VLANs:

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

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

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

A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs.
VLAN trunks facilitate inter-switch communication by carrying traffic associated with multiple VLANs. IEEE 802.1Q frame tagging differentiates between Ethernet frames associated with distinct VLANs as they traverse common trunk links. To enable trunk links, use the **switchport mode trunk** command. Use the **show interfaces trunk** command to check whether a trunk has been established between switches.
Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis only, between network devices. DTP is a Cisco proprietary protocol that is automatically enabled on Catalyst 2960 and Catalyst 3560 Series switches.
To place a switch into its factory default condition with 1 default VLAN, use the commands **delete flash:vlan.dat** and **erase startup-config.**
This chapter also examined the configuration, verification, and troubleshooting of VLANs and trunks using the Cisco IOS CLI.
Inter-VLAN routing is the process of routing traffic between different VLANs, using either a dedicated router or a multilayer switch. Inter-VLAN routing facilitates communication between devices isolated by VLAN boundaries.
Legacy inter-VLAN routing depended on a physical router port being available for each configured VLAN. This has been replaced by the router-on-a-stick topology that relies on an external router with subinterfaces trunked to a Layer 2 switch. With the router-on-a-stick option, appropriate IP addressing and VLAN information must be configured on each logical subinterface and a trunk encapsulation must be configured to match that of the trunking interface of the switch.

Layer 3 switching using Switch Virtual Interfaces (SVIs) is a method of inter-VLAN routing that can be configured on Catalyst 2960 switches. An SVI with appropriate IP addressing is configured for each VLAN and provides Layer 3 processing for packets to or from all switch ports associated with those VLANs.
Another method of Layer 3 inter-VLAN routing is using routed ports. A routed port is a physical port that acts similarly to an interface on a router. Routed ports are mostly configured between switches in the core and distribution layer.
Troubleshooting inter-VLAN routing with a router or a Layer 3 switch are similar. Common errors involve VLAN, trunk, Layer 3 interface, and IP address configurations.

Section 6.1

New Terms and Commands

• VLAN • Logical broadcast domain • Data VLAN • Default VLAN • Native VLAN • Management VLAN • **show vlan brief** • Voice VLAN • VLAN Trunk • VLAN Segmentation • IEEE 802.1Q • VLAN Tagging • Canonical Format Identifier (CFI)	• User Priority • VLAN ID • Type • **show interfaces** *int* **switchport**

New Terms and Commands

Section 6.2

New Terms and Commands

• Normal Range VLANs • Extended Range VLANs • **vlan** *vlan-id* • **name** *vlan-name* • **switchport mode access** • **switchport access vlan** *vlan-id* • **interface range** • **no switchport access vlan** *vlan-id* • **no vlan** *vlan-id* • **delete flash:vlan.dat** • **delete vlan.dat**	• **show vlan** • **show interfaces** • **show vlan summary** • **show interfaces vlan** *vlan_id* • **switchport mode trunk** • **switchport trunk allowed vlan** *vlan_list* • **switchport trunk native vlan** *vlan_id* • **no switchport trunk allowed vlan** • **no switchport trunk native vlan** • **show interfaces switchport**	• **no switchport access vlan** *vlan_id* • **show interfaces trunk** • **show interfaces** *int_id* **trunk**

New Terms and Commands

Section 6.3

New Terms and Commands

- Legacy Inter-VLAN Routing
- Router-on-a-Stick Inter-VLAN Routing
- **interface** *interface_id.subinterface_id*
- **encapsulation dot1q** *vlan_id*
- IEEE 802.1Q

New Terms and Commands