Module 2: VLANs

COURSE OVERVIEW

Course No.	**CCNA301/CCNA301L**
Course Code	IF-3-A-3, IF-3-A-4, IF-3-B-3, IF-3-B-4
Descriptive Title	ROUTERS AND ROUTING BASIC
Credit Units	2 unit lecture / 1 unit lab
School Year/Term	1st Semester, AY: 2021-2022
Mode of Delivery	Asynchronous, Synchronous
Name of Instructor/ Professor	Czarina Ancella G. Gabi
Course Description	This course describes the architecture, components, and operations of routers and switches in a small network. Students learn how to configure a router and a switch for basic functionality. By the end of this course, students will be able to configure and troubleshoot routers and switches and resolve common issues with static route, RIPv2 in networks.
Course Outcomes	***Knowledge (Think)*** Apply skills on VLAN segmentation and inter-VLAN routing ***Skills (Do)*** Demonstrate knowledge and skills on basic router configuration Perform static and dynamic routing in a small to medium-sized networks ***Heart (Feel)*** Express importance of adopting a scalable network design
SLSU Vision	A high quality corporate university of Science, Technology and Innovation
SLSU Mission	SLSU will: 1. Develop Science, Technology and Innovation leaders and professionals 2. Produce high-impact technologies from research and innovations 3. Contribute to sustainable development through responsive community engagement programs; 4. Generate revenues to be self-sufficient and financially-viable

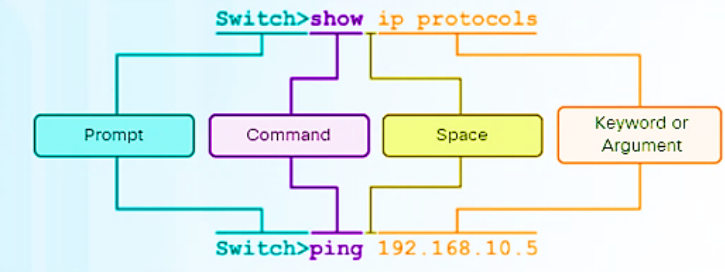
Welcome! The goal of this course is to introduce you to networking concepts and technologies that facilitates to scale network easily. This instructional material will assist you in developing the skills necessary to plan and implement small networks supporting a range of applications.

Because of COVID-19, we are implementing "Flexible Learning" in SLSU. With this, you can now study at your own pace, anytime, and anywhere. In addition, online classes will be conducted. To those with no available device or internet connection, a hard copy of this module will be provided to you. For activities like practical exercises/simulations, traditional (paper and pen) means may be used but if laptop/PC is available, a Packet Tracer software may be installed to perform the exercises. An online, downloadable version of this will also be made available for those with devices and internet access. You can use your smart phone, tablet, laptop, or desktop to access the module, read or review text, and practice using interactive media. Included in the modules are Quick Reviews which are meant to self-assess your learnings. However, your results to these reviews will not be recorded.

Since this is your second CCNA course, you will be learning new commands. Thus, be reminded of the basic IOS command structure as well as the syntax conventions used. In the module, the newly-introduced syntaxes follow the example configurations.

Basic IOS Command Structure

A Cisco IOS device supports many commands. Each IOS command has a specific format or syntax and can only be executed at the appropriate mode.



The syntax for a command is the command followed by any appropriate keywords and arguments.

- **Keyword** - a specific parameter defined in the operating system (in the figure, **ip protocols**)
- **Argument** - not predefined; a value or variable defined by the user (in the figure, **192.168.10.5**)

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets indicate an optional element (keyword or argument).
{x}	Braces indicate a required element (keyword or argument).
[x {y | z}]	Braces and vertical lines within square brackets indicate a required choice within an optional element.

To enroll to our course, open https://you.slsuonline.edu.ph of SLSU's Flexible Learning Management System (FLMS). Login your Moodle accounts and look for Routers and Routing Basic course. Finally, input the access code "CCNA301/L" upon enrolment. Modules and assessments will be provided at Moodle. A Google Meet link will be provided to you before the conduct of online classes. Likewise, you are enjoined to join our Facebook group facebook.com/groups/ccna3012021 for announcements and instructions.

SLSU is a Cisco Local Academy. All the content including the figures and examples, and some activities in this module are taken from the Cisco Networking Academy.

Course Objective: Apply knowledge on VLAN segmentation and inter-VLAN Routing

Intended Learning Outcome:
ILO2. Familiarize various VLAN-related terminologies and its types
ILO7. Practice VLAN implementation and trunking.
ILO9. Demonstrate inter-VLAN routing

INTRODUCTION

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.

As the number of switches increases on a small- or medium-sized business network, the overall administration required to manage VLANs and trunks in a network becomes a challenge. This module will examine some of the strategies and protocols that can be used to manage VLANs.

Terms and Commands

- VLAN
- Normal Range VLANs
- Extended Range VLANs
- IEEE 802.1Q
- Data VLAN
- Default VLAN
- Native VLAN
- Voice VLAN
- Management VLAN
- Legacy Inter-VLAN Routing
- Router-on-a-Stick Inter-VLAN Routing
- **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**
- **interface** *interface_id.subinterface_id*
- **encapsulation dot1q** *vlan_id*

DISCUSSION ON MODULE 2: VLANs

Lesson 1. VLAN Segmentation

Overview of VLANs: VLAN Definitions

Within a switched network, **VLANs** provide segmentation and organizational flexibility. **VLANs** provide a way to group devices within a LAN as shown in Figure 1. 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.

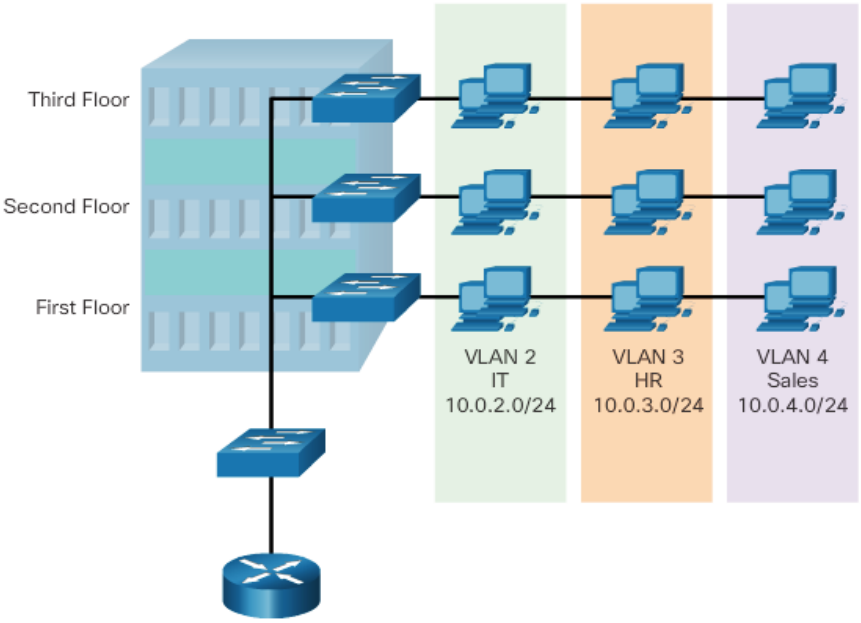


Figure 1. Defining VLAN groups (example)

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

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 2.

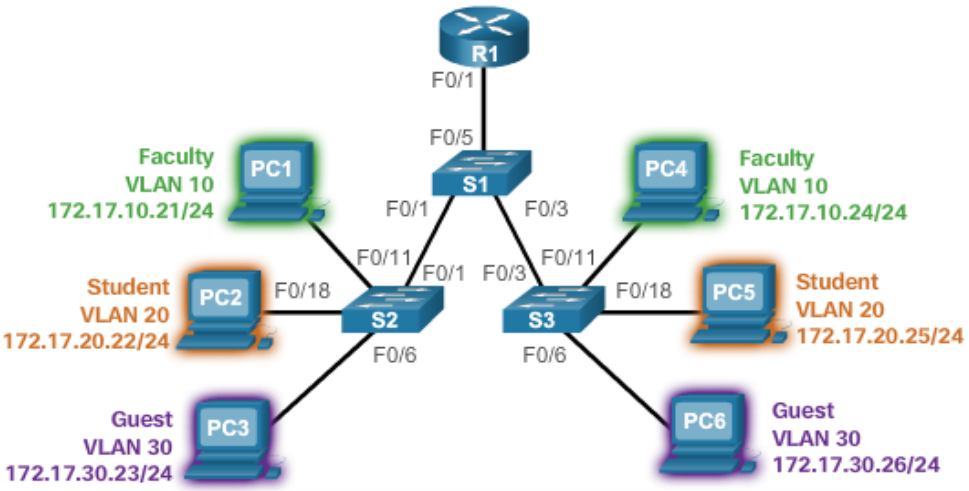


Figure 2. VLAN segmentation (example)

Overview of VLANs: 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 Figure 3, 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.

```
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
```

Figure 3. Show VLAN brief output (for default VLAN)

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 Figure 3, 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 VLAN

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 150ms across the network

To meet these requirements, the entire network has to be designed to support VoIP.

In Figure 4, VLAN 150 is designed to carry voice traffic. The student computer PC5 is attached to the Cisco IP phone, and the phone is attached to switch S3. PC5 is in VLAN 20, which is used for student data.

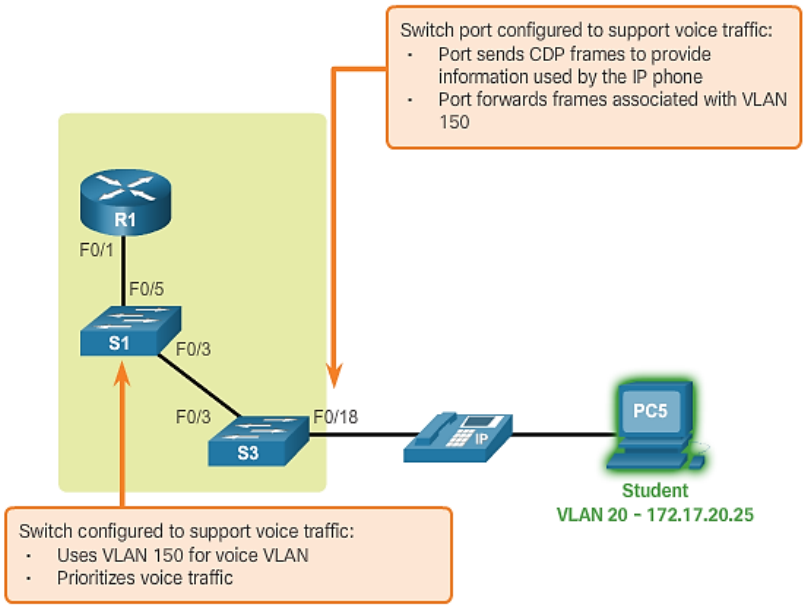


Figure 4. Voice VLAN

VLANs in a Multi-Switched Environment: 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 Figure 5, the links between switches S1

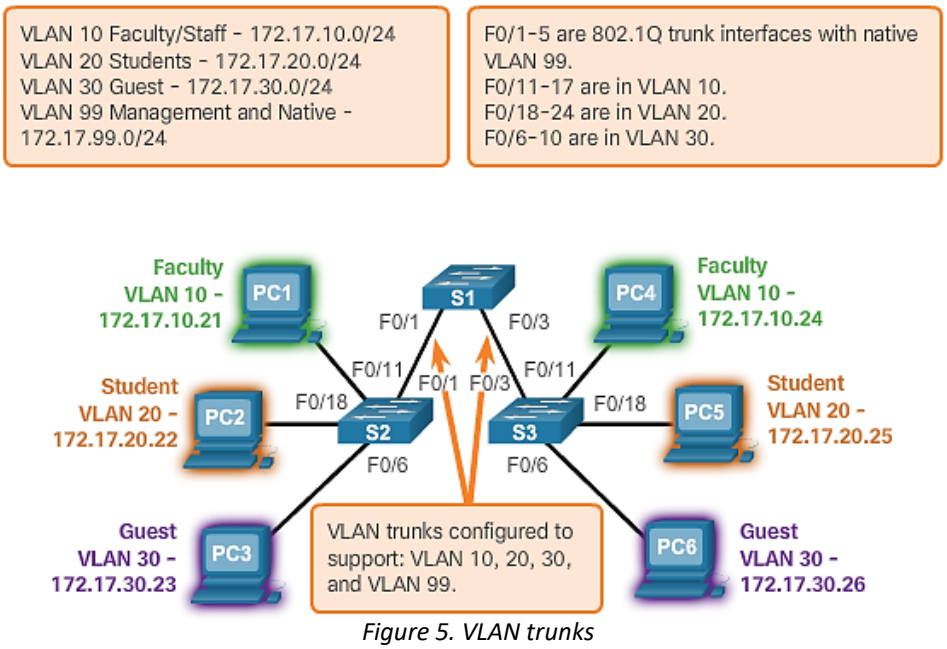


Figure 5. VLAN trunks

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

In normal operation, when a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports except the port where the broadcast was received. In Figure 6A, the entire network is configured in the same subnet (172.17.40.0/24) and no VLANs are configured. As a result, when the faculty computer (PC1) sends out a broadcast frame, switch S2 sends that broadcast frame out all of its ports. Eventually the entire network receives the broadcast because the network is one broadcast domain.

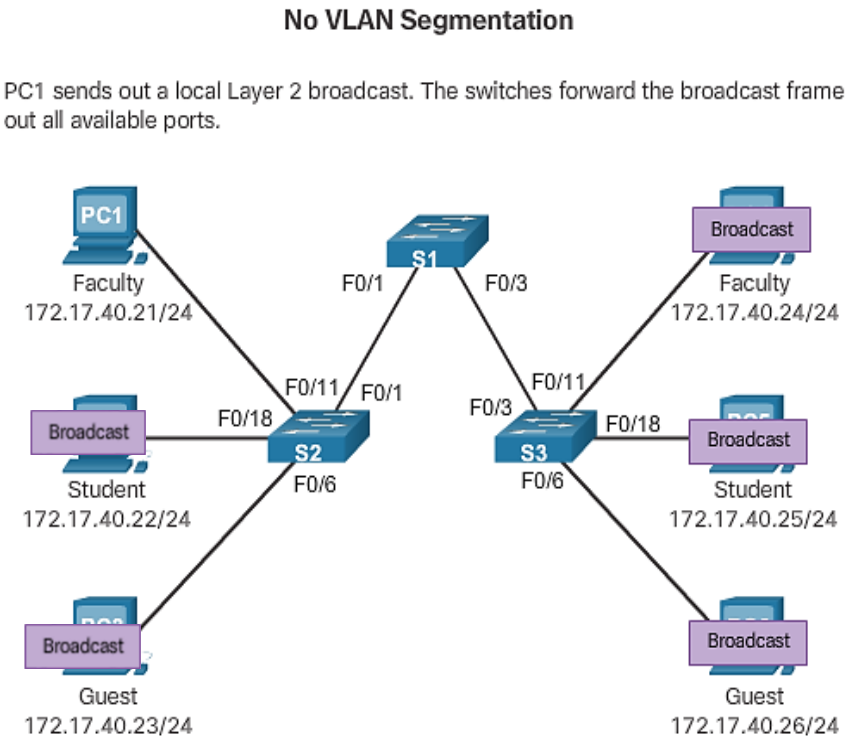


Figure 6A. Broadcast domain for NO VLAN SEGMENTATION

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

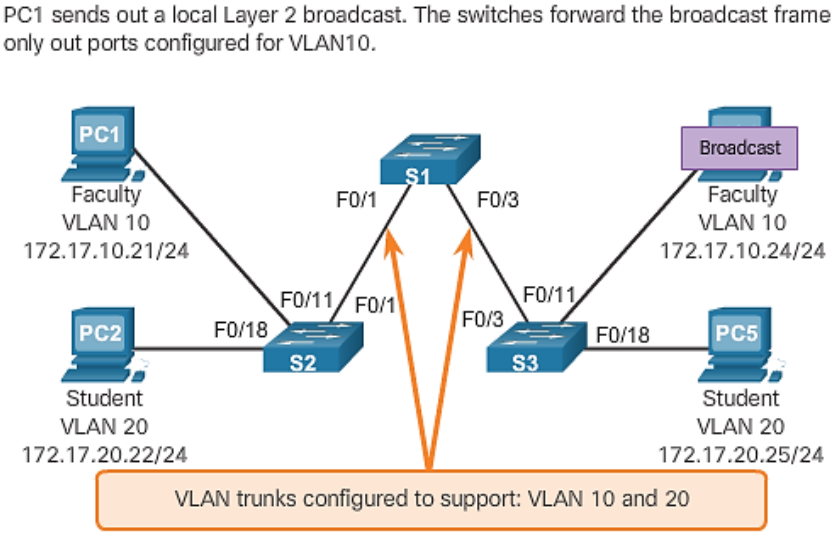


Figure 6B. Broadcast domain for WITH VLAN SEGMENTATION

VLANs in a Multi-Switched Environment: Tagging Ethernet Frames for VLAN Identification

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. Switches tag frames to identify the VLAN to which they belong.

Different tagging protocols exist; IEEE 802.1Q is a very popular example. The protocol defines the structure of the tagging header added to the frame. Switches add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports. When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.

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 as shown in Figure 7:

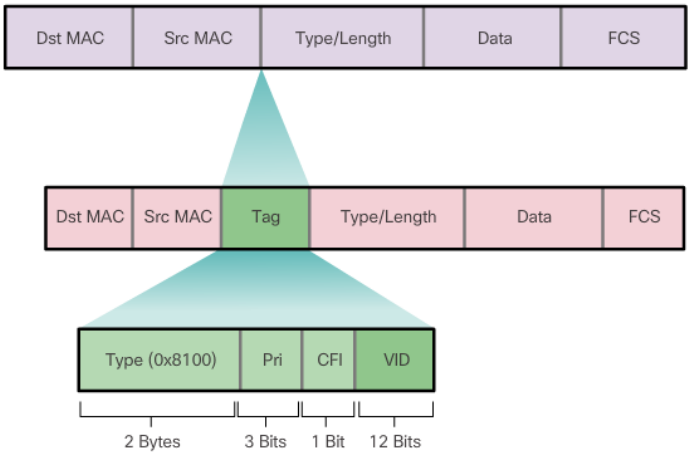


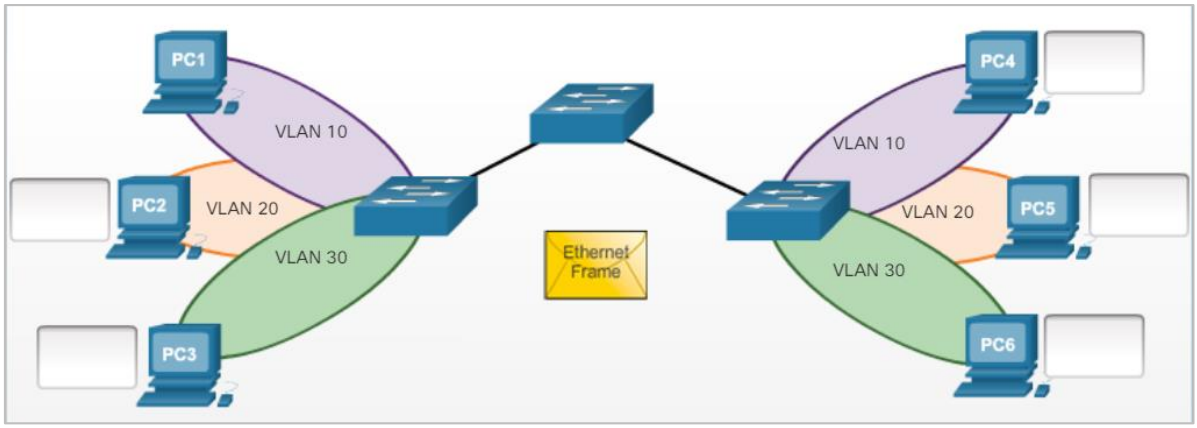
Figure 7. Fields in Ethernet 802.1Q frame

- **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.

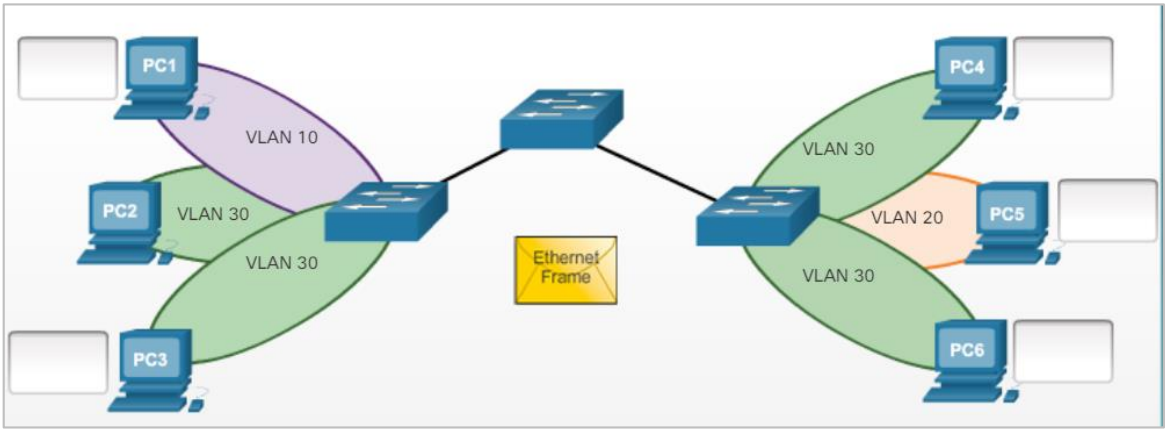
Quick review: Converged Networks - Identify Switched Network Terminology

Instruction: Select which device or devices will receive the frame based on the scenario given.

1. PC1 sends a broadcast message. Which PC(s) will receive a copy of the broadcast frame?



2. PC2 sends a broadcast message. Which PC(s) will receive a copy of the broadcast frame?



Lesson 2. VLAN Implementation

VLANs in a Multi-Switched Environment: Tagging Ethernet Frames for VLAN Identification

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. Figure 8 illustrates the available VLANs on a Catalyst 2960 switch running Cisco IOS Release 15.x.

```
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
```

Figure 8. Show vlan brief (example of normal range VLANs)

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

Figure 9 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.

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`

Figure 9. Syntax for VLAN creation

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

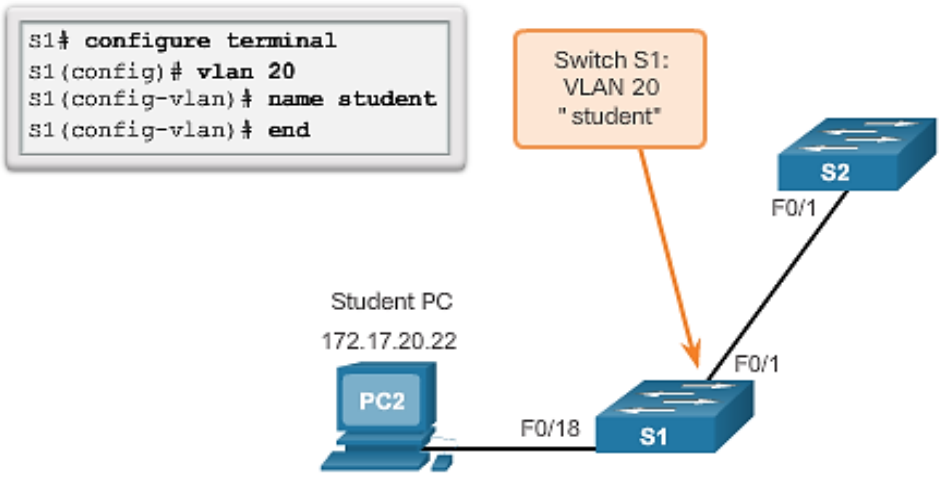


Figure 10. VLAN creation (sample)

VLAN Assignment: Assigning Ports to VLANs

After creating a VLAN, the next step is to assign ports to the VLAN. Figure 11 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.

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**

Figure 11. VLAN creation (sample)

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

In the example in Figure 12, 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.

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

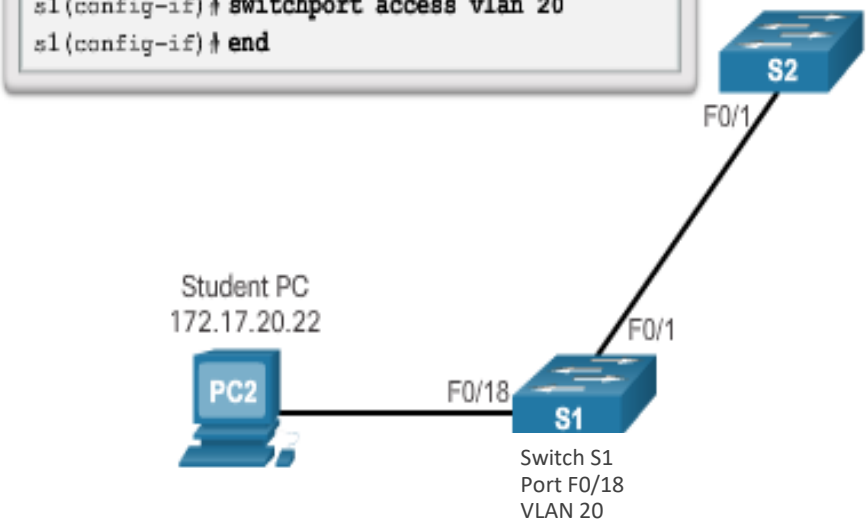


Figure 12. Port assignment to VLAN (sample)

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
```

Consider the topology in Figure 13. 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.

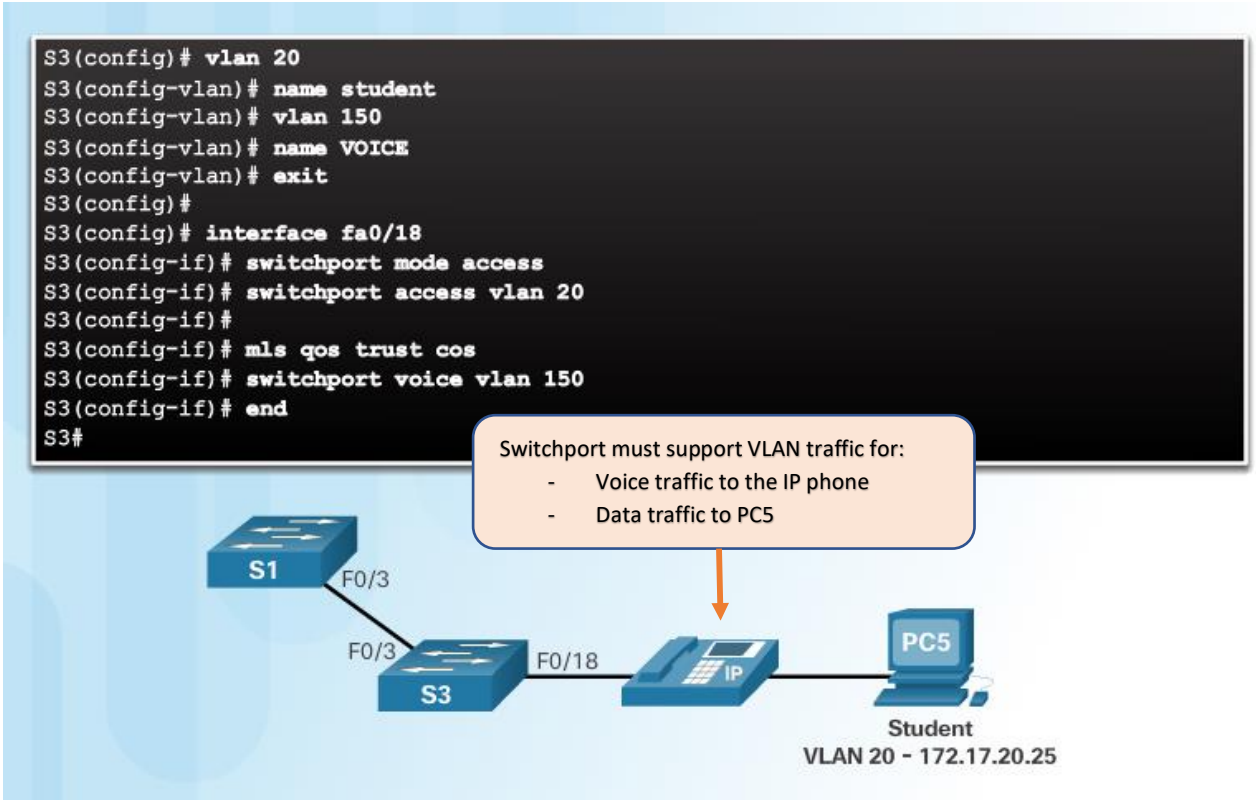


Figure 13. Port assignment to VLAN (sample with IP phone)

The configuration in Figure 13 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.

VLAN Assignment: Changing VLAN Port Membership

Figure 14 shows the syntax for changing a switch port to VLAN 1 membership with the **no switchport access vlan** interface configuration mode command.

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

Figure 14. Syntax to remove VLAN assignment

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 15. 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.

```
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#
```

Figure 15. Remove VLAN assignment (sample)

VLAN 20 is still active (refer to Figure 15), even though no ports are assigned to it. In Figure 16, the **show interfaces F0/18 switchport** output verifies that the access VLAN for interface F0/18 has been reset to VLAN 1.

```
S1# sh interfaces F0/18 switchport
Name: F0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

<output omitted>
```

Figure 16. Verify VLAN assignment of F0/18

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 (Figure 17).

```
S1# config t
S1(config)# interface F0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name                Status    Ports
---- ----------------- -------- -------------------------------
1    default              active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                   Gi0/2
20   student              active   F0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Figure 17. Change VLAN membership

VLAN Assignment: Deleting VLAN

In Figure 18, 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.

```
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#
```

Figure 18. Delete a VLAN

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

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

Figures 19A and 19B display the **show vlan** and **show interfaces** command options respectively.

show vlan Command

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

Figure 19A. Show VLAN

show interfaces Command

Cisco IOS CLI Command Syntax	
show interfaces [*interface-id* | **vlan** *vlan-id*] | **switchport**	
Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 6.	*interface-id*
VLAN identification. The range is 1 to 4094.	**vlan** *vlan-id*
Display the administrative and operational status of a switching port, including port blocking and port protection settings.	**switchport**

Figure 19B. Show interfaces

In the example in Figure 20, 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 20 shows seven VLANs.

```
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#
```

Figure 20. Show VLAN name

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 21, indicating that VLAN 20 is up.

```
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
```

Figure 21. Show interfaces VLAN

VLAN Trunks: 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. The syntax is provided in Figure 22. A sample topology and its trunk configuration are presented in Figures 23 and 24, respectively.

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.

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`

Figure 22. Syntax to enable trunk links

```
VLAN 10 - Faculty/Staff - 172.17.10.0/24
VLAN 20 - Students - 172.17.20.0/24
VLAN 30 - Guest - 172.17.30.0/24
VLAN 99 - Native - 172.17.99.0/24
```

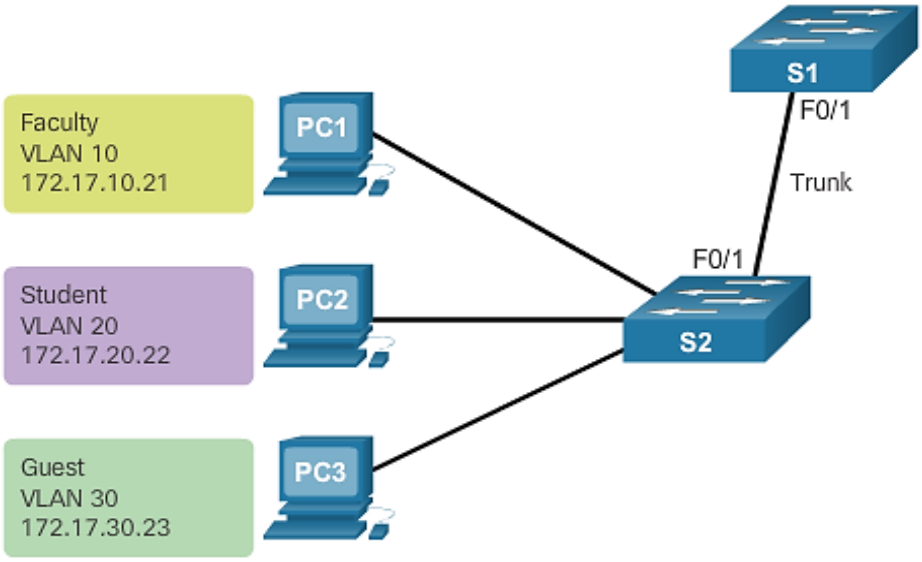


Figure 23. Sample topology

```
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
```

Figure 24. Trunk configuration

VLAN Trunks: Resetting the Trunk to Default State

Figure 25 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.

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`

Figure 25. Syntax to reset trunk to default state

Figure 26 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.

```
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>
```

Figure 26. reset trunk to default state configuration

In Figure 27, 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.

```
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>
```

Figure 27. Verify port setting

VLAN Trunks: Trunk Verification

Figure 28 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.

```
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>
```

Figure 28. Verify trunk configuration

Troubleshoot VLANs and Trunks: 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 29, PC1 cannot connect to the Web/TFTP server shown.

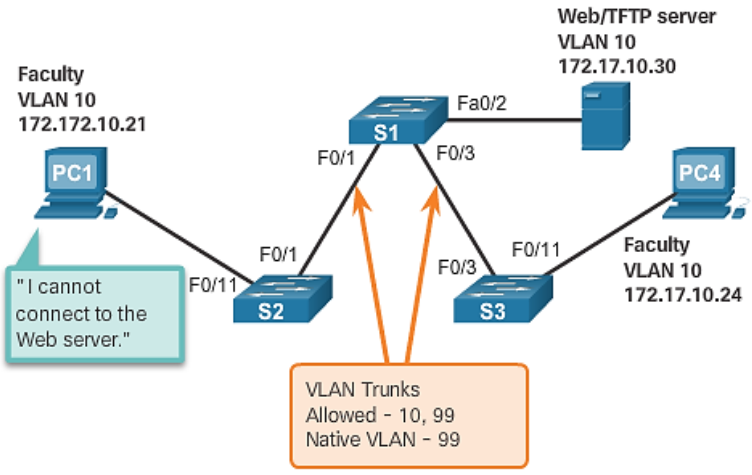


Figure 29. Problem 1: IP issue with VLAN

A check of the IPv4 configuration settings of PC1 shown in Figure 30, 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.

```
PC1> ipconfig

IP Address.....................: 172.172.10.21
Subnet Mask....................: 255.255.0.0
Default Gateway................: 0.0.0.0

PC1>
```

Figure 30. Output from PC 1

In Figure 31, the PC1 Fast Ethernet configuration dialog box shows the updated IPv4 address of 172.17.10.21. The output shown in Figure 32 reveals that PC1 has regained connectivity to the Web/TFTP server found at IPv4 address 172.17.10.30.

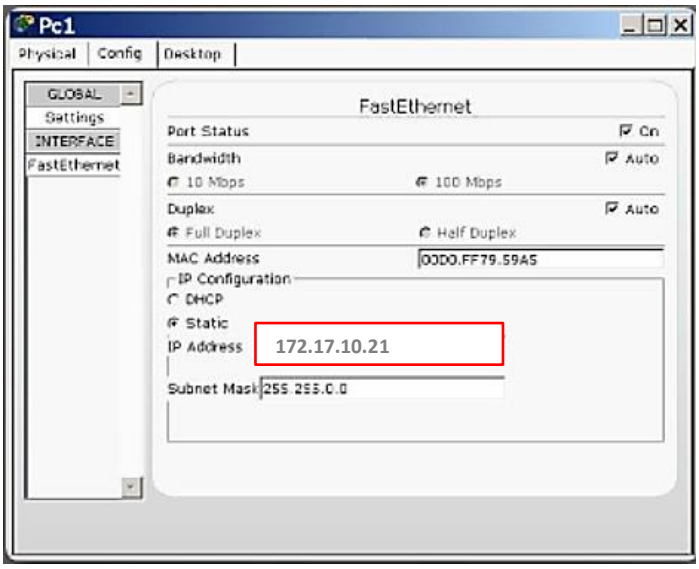


Figure 31. Solution: Change IP address of PC1

```
PC1> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: Bytes=32 Time=147ms TTL=128
```

Figure 32. Output from PC1 after correction

Troubleshoot VLANs and Trunks: 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 33 to troubleshoot:

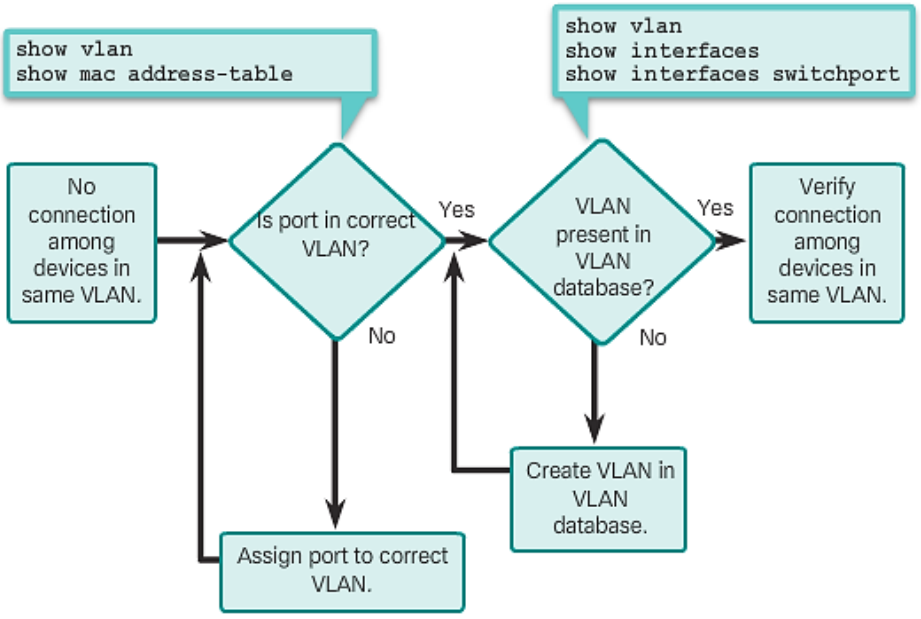


Figure 33. Solution: Change IP address of PC1

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 shown in Figure 34.

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 35.

The example in Figure 34 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.

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
10     000c.296a.a21c    DYNAMIC     Fa0/1
10     000f.34f9.9181    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 2
```

Figure 34. MAC addresses learned on the F0/1 interface

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.

```
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
```

Figure 35. verify inactive port

Troubleshoot VLANs and Trunks: 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.

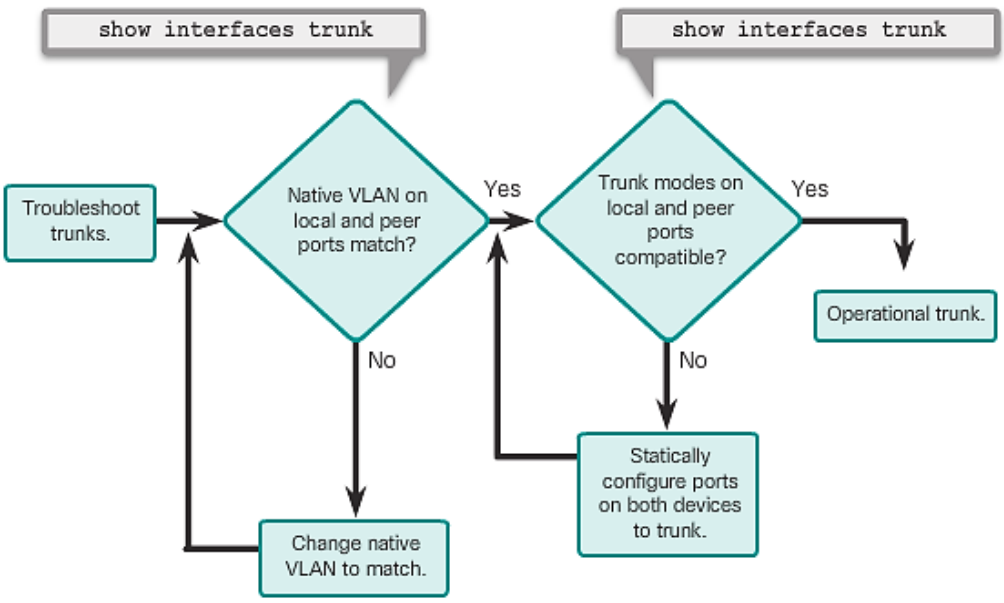


Figure 36. Verify inactive port

Figure 36 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 37 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 37, 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.

```
SW1# show interfaces f0/1 trunk

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

<output omitted>
```

Figure 37. Native VLAN Mismatch issue

Troubleshoot VLANs and Trunks: 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 shown in Figure 38 are the most common:

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, both local and peer switchport modes are configured as dynamic auto.
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.

Figure 38. Common Problem with Trunks

Troubleshoot VLANs and Trunks: 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 39, PC4 cannot connect to the internal web server. The topology indicates a valid configuration. Why is there a problem?

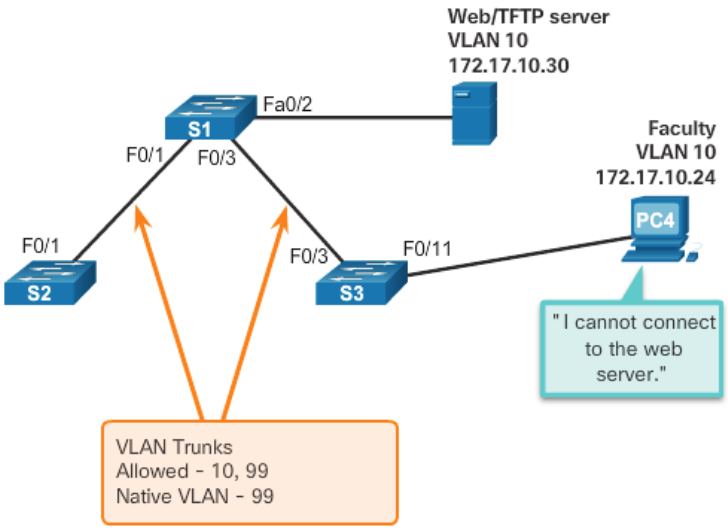


Figure 39. Scenario topology

Using the **show interfaces trunk command,** the output shown in Figure 40A 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.

However, shown in Figure 40B is 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.

```
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
```

Figure 40A. Output from S1

```
S3# show interfaces trunk

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

Figure 40B. Output from S3

To resolve the issue, reconfigure the trunk mode of the F0/3 ports on switch S3, as shown in Figure 41A. After the configuration change, the output of the **show interfaces** command shown in Figure 41B indicates that the port on switch S3 is now in trunking. The **ping** output from PC4 shown in Figure 41C indicates that it has regained connectivity to the Web/TFTP server found at IPv4 address 172.17.10.30.

```
S3# config terminal
S3(config)# interface f0/3
S3(config-if)# switchport mode trunk
S3(config-if)# end
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
…
S3# show interfaces trunk
Port     Mode         Encapsulation  Status     Native vlan
Fa0/3    on           802.1q         trunking   99
Port     Vlans allowed on trunk
Fa0/3    10,99
Port     Vlans allowed and active in management domain
Fa0/3    10,99
Port     Vlans in spanning tree forwarding state and not pruned
Fa0/3    10,99
S3#
```

Figure 41A. Output from S1

```
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
…
```

Figure 41B. Corrected trunk mode on S1

```
PC4> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
…
```

Figure 41C. ping output from PC4

Troubleshoot VLANs and Trunks: 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 43, VLAN 20 (Student) and PC5 have been added to the network. The documentation has been updated to show that the VLANs allowed on the trunk are 10, 20, and 99. In this scenario, PC5 cannot connect to the student email server.

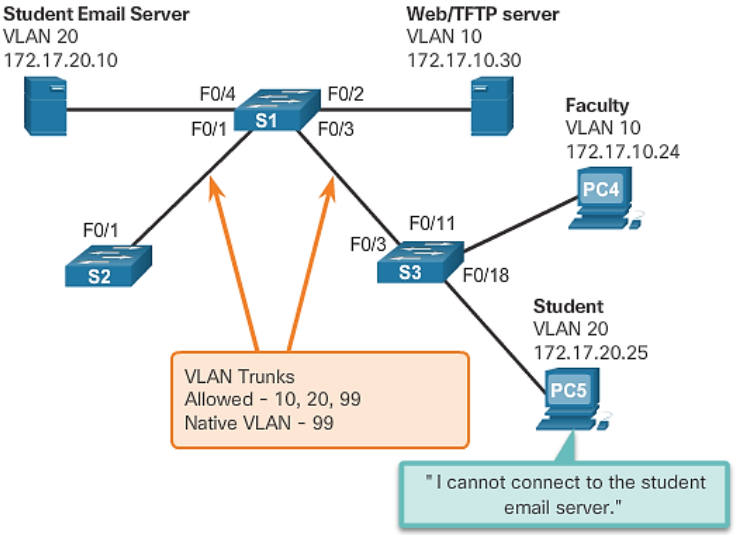


Figure 43. Scenario topology

The **show interfaces trunk** command shown if Figure 44 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 (shown in Figure 45) 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.

```
S3# show interfaces trunk
Port  Mode  Encapsulation  Status    Native vlan
Fa0/3 on    802.1q         trunking  99
Port  Vlans allowed on trunk
Fa0/3 10,20,99
Port  Vlans allowed and active in management domain
Fa0/3 10,20,99
Port  Vlans in spanning tree forwarding state and not
pruned
Fa0/3 10,20,99
```

Figure 44. Output from S3

```
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#
```

Figure 45. Output from S1

Reconfigure F0/1 and F0/3 on switch S1 using the **switchport trunk allowed vlan 10,20,99** command as shown in Figure 46. The output shows that VLANs 10, 20, and 99 are now added to the F0/1 and F0/3 ports on switch S1. Using **ping** (Figure 47), PC5 has regained connectivity to the student email server found at IPv4 address 172.17.20.10.

```
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
```

Figure 46. Output from S1

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

Figure 47. Ping output from PC5

Lesson 3. Inter-VLAN Routing Using Routers

Inter-VLAN Routing Operation: What is Inter-VLAN Routing?

A VLAN is a broadcast domain, so computers on separate VLANs cannot communicate without the assistance of a router. Layer 2 switches have very limited IPv4 and IPv6 functionality and cannot perform the dynamic routing function of routers. 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*** *(Figure 48).*

There are three options for inter-VLAN routing:

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

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

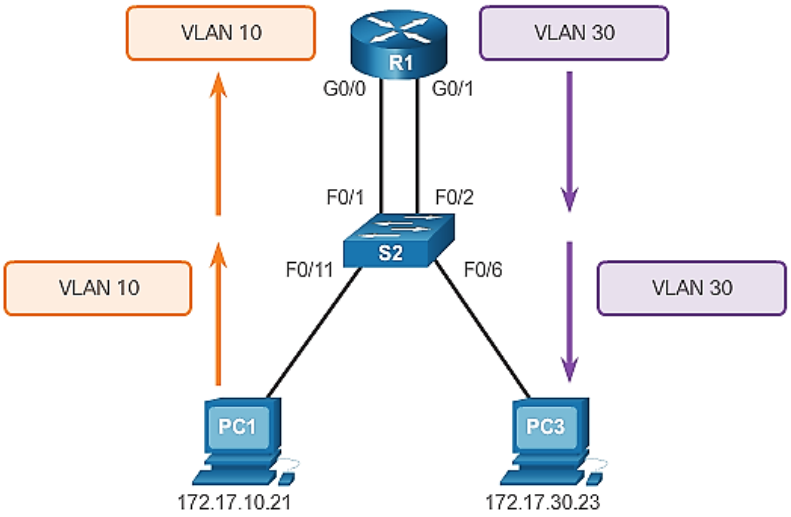


Figure 48. Inter-VLAN routing

Inter-VLAN Routing Operation: 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.

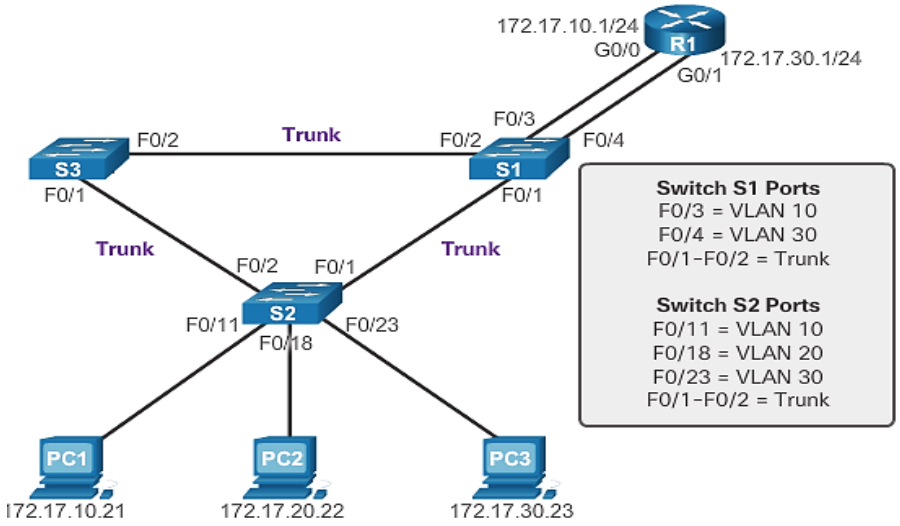


Figure 49. Legacy Inter-VLAN routing (example)

In this **legacy** approach shown in Figure 49, 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.

Configure Legacy Inter-VLAN Routing: Configure Legacy Inter-VLAN Routing: Switch Configuration

To configure legacy inter-VLAN routing, start by configuring the switch. Refer to Figure 50 for the scenario topology.

As shown in the figure, R1 is connected to switch ports F0/4 and F0/5 on switch S1, which have been configured for VLANs 10 and 30, respectively.

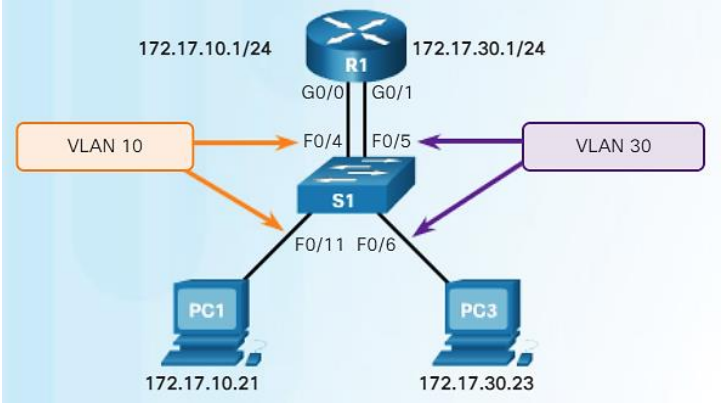


Figure 50. Scenario topology

Use the **vlan** *vlan_id* global configuration mode command to create VLANs. In this example, VLANs 10 and 30 were created on switch S1 as shown in Figure 51.

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.

```
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
```

Figure 51. Legacy Inter-VLAN Routing: Switch Configuration

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: Configure Legacy Inter-VLAN Routing: Router 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.

```
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, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```

Figure 52. Legacy Inter-VLAN Routing: Router Configuration

As shown in Figure 52, 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. Once issued, a notification is displayed (Figure 52), 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 now capable of performing inter-VLAN routing.

```
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
L        172.17.10.1/32 is directly connected, GigabitEthernet0/0
C        172.17.30.0/24 is directly connected, GigabitEthernet0/1
L        172.17.30.1/32 is directly connected, GigabitEthernet0/1
```

Figure 53. Legacy Inter-VLAN Routing: Router Configuration

Figure 53 examines the routing table using the **show ip route** command. In the figure, 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.

Inter-VLAN Routing Operation: Router-on-a-Stick Inter-VLAN Routing

'**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 Figure 54, the router is connected to switch S1 using a single, physical network connection (a trunk). Router interface configured to operate as a trunk link and is connected to a trunked switch port. 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 sub-interfaces. 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.

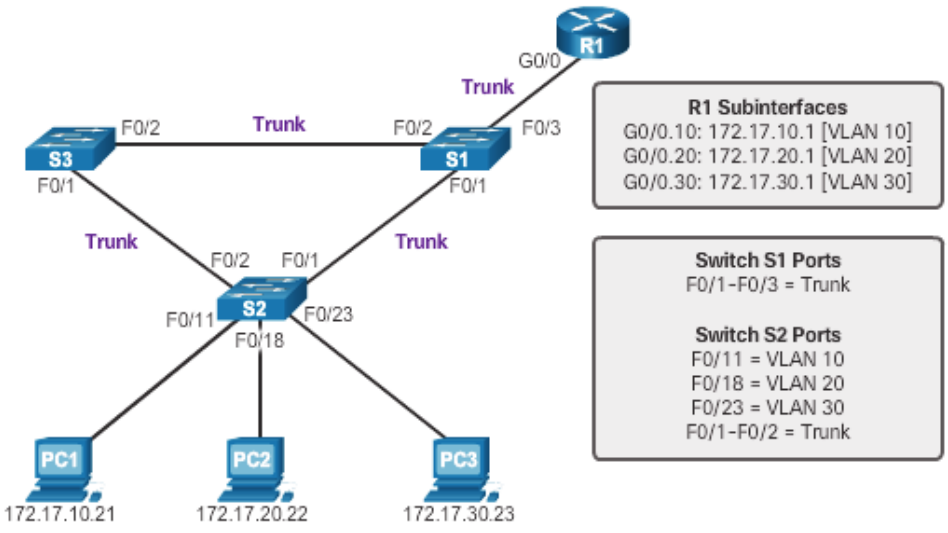


Figure 54. Router-on-a-Stick Inter-VLAN Routing

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.

In Figure 55, router R1 is connected to switch S1 on trunk port F0/5. VLANs 10 and 30 are created/added to switch S1 (Figure 56).

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 (Figure 56).

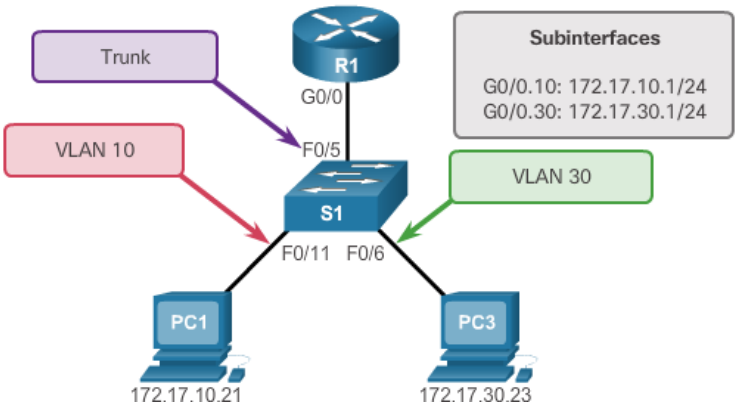


Figure 55. Scenario topology

```
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#
```

Figure 56. Configure Router-on-a-Stick: Switch Subinterface

Configure Router-on-a-Stick Inter-VLAN Routing: Configure Router-on-a-Stick: Sub-interface Configuration

The configuration of the router is different when a router-on-a-stick configuration is used, compared to legacy inter-VLAN routing. Figure 57 shows that multiple sub-interfaces are configured.

```
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
```

Figure 57. Configure Router-on-a-Stick: Router Subinterface Configuration

Each subinterface is created using the **interface** *interface_id.subinterface_id* *at* global configuration mode command. The syntax for the sub-interface is the physical interface, in this case g0/0, followed by a period and a subinterface 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 (Figure 57), 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.

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.

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.

In Figure 58, 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.

```
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>
```

Figure 58. Verify sub-interfaces – show VLAN

Examine the routing table using the **show ip route** command (Figure 59). 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.

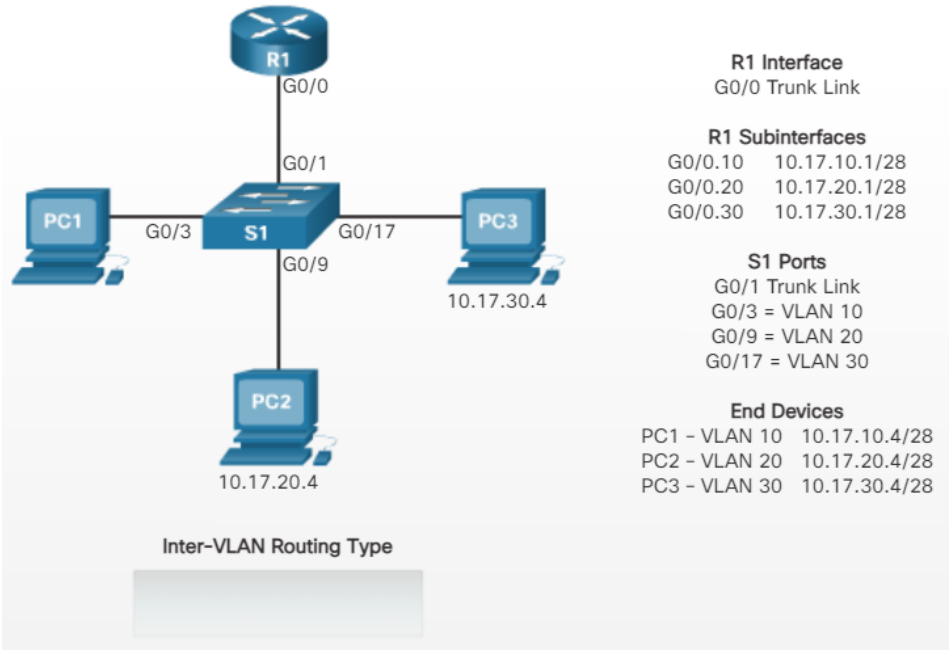
```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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
```

Figure 59. Verify sub-interfaces – show IP route

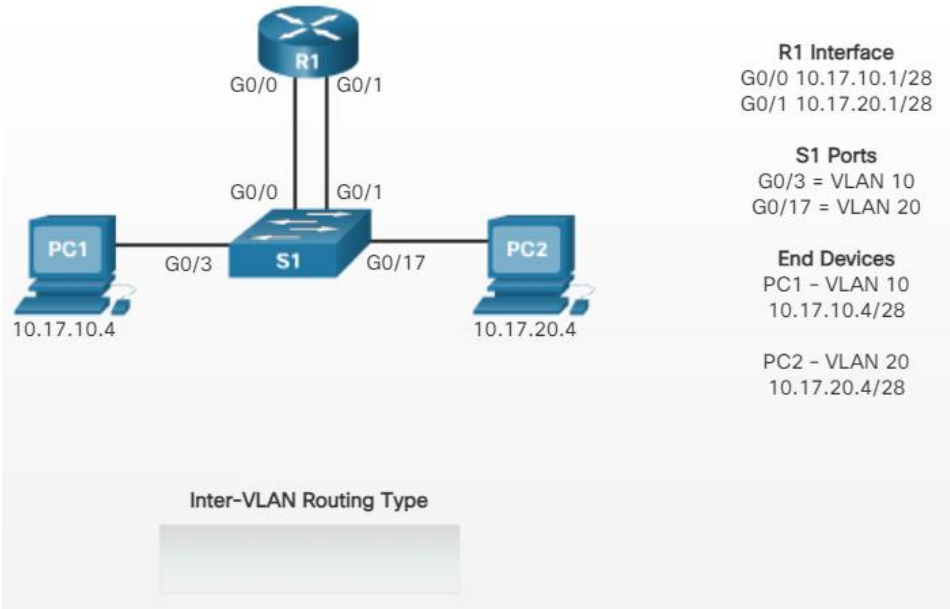
Quick review: Inter-VLAN Routing - Identify the Type of Inter-VLAN Routing

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

1.



2.



Summary

This module 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 module 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.

REFERENCES

Electronic Resource:

1. Cisco Networking Academy [internet]. [cited 16 August 2021]. Available from: www. netacad.net

Books:

1. Cisco Networking Academy. Router and Routing Basic: Companion Guide. Singapore: Pearson Education South Asia Pte Ltd. 2014.
2. Cisco Networking Academy. Router and Routing Basic: Lab manual. Singapore: Pearson Education South Asia Pte Ltd. 2014.

For questions and clarifications, please contact:

CZARINA ANCELLA G. GABI, PhD
Assistant Professor IV
Southern Leyte State University
Sogod, Southern Leyte
Mobile Number: +63 9173088375
Email Address: czaguasa@gmail.com
Facebook: facebook.com/czaguasa