Alan Palayil

ECE 407

ECE 407

Introduction to Computer Networks Laboratory

Practice 5 – Port Based Virtual Local Area Networks

Objectives

The goal of this experiment is to:

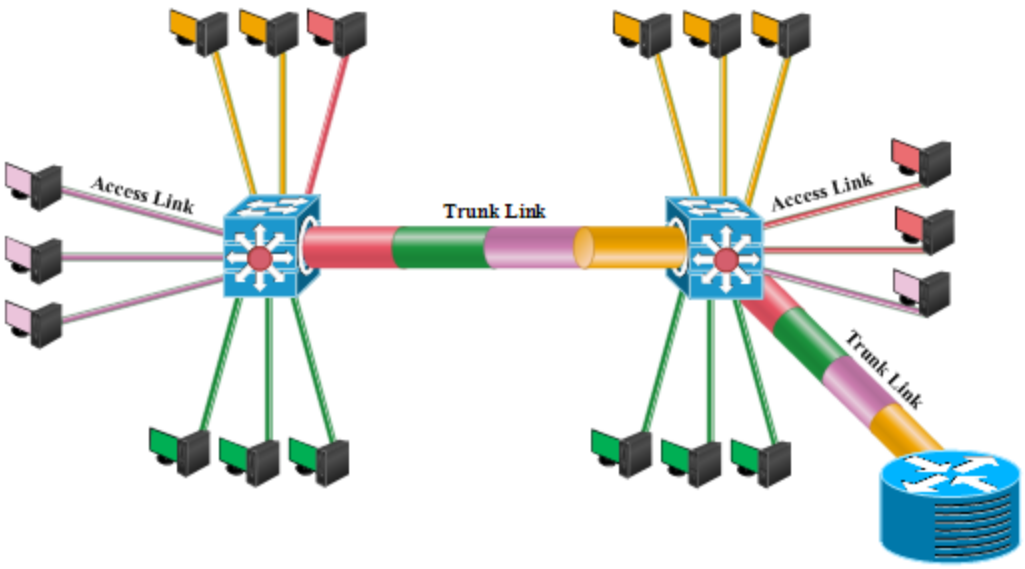
1. Familiarize students with named and numbered standard Access Control Lists (ACLs).
2. Familiarize students with named and numbered extended ACLs.

Background

Modern switches use virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones. By separating hosts into different networks, VLANs can be used to control which hosts can communicate, which also provides a security measure.

When a switch receives data from a LAN segment on a certain port, it implicitly tags the data with a VLAN identifier associated with that switch port. This tagging also determines to which VLAN the data received belongs. The connection between the LAN segment and the switch is called an access link, because it connects a VLAN-unaware device (LAN segment) to the port of a VLAN-aware device (switch). All frames on access links are implicitly tagged (i.e., there is no tagging information in the packet header, yet tag information is implicitly known to the switch through its VLAN port mapping). VLAN trunk links on the other hand, are used to span VLANs across multiple devices. Trunks allow the traffic from multiple VLANS to travel over a single link, while keeping the VLAN identification and segmentation intact. To this end, the 802.1Q tagging protocol is used to explicitly tag the frames with their VLAN ID before they travel on a trunk link. The IEEE 802.1Q header contains a 4-byte tag header containing a 2-byte tag protocol identifier (TPID) and a 2-byte tag control information (TCI). The TPID has a fixed value of 0x8100 that indicates that the frame carries the 802.1Q/802.1p tag information. After a frame has traversed a trunk link, the switch on the other side will remove the 802.1Q tag and forward the frame to access port(s) which belong to the same VLAN ID. Only frames traversing a trunk link are explicitly tagged with their VLAN ID. Note that if the frame has a VLAN ID equal to the default native VLAN, it is sent untagged.

Exercises in this experiment are based on Cisco NetAcad Labs



Types of Port-Based VLANs

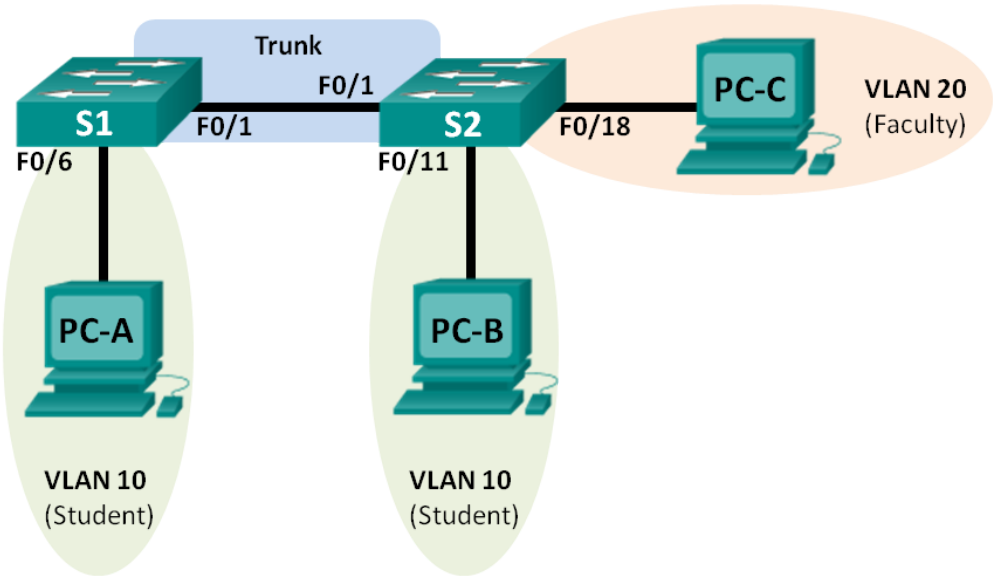
- Data VLAN: only carries user-generated traffic.
- Default VLAN: the VLAN that all switch ports become part of after the initial boot up of the switch. By default, VLAN 1 is the default VLAN.
- Management VLAN: a VLAN which is configured to access the switch virtual interface (SVI), to manage the switch. The management VLAN should be assigned an IP address and subnet mask.
- Native VLAN: native VLAN is used to allow untagged frames (frames coming from ports without a VLAN ID, i.e., VLAN ID is that of the default VLAN) to traverse the 802.1Q trunk link. Default native VLAN is VLAN 1. Note that if an 802.1Q trunk port receives a tagged frame on the native VLAN, it drops the frame. This happens when a trunk port is connected to devices from other vendors, which tag frames with the native VLAN.

Routing traffic between VLANs

1. Per-interface inter-VLAN routing: a Cisco router with two ethernet interfaces connects to both VLANs with an appropriate IP address assigned to each interface. IP routing is of course enabled on the router. Additionally, each host should use the router's interface connected to their network as a default gateway. Observe that this scenario is not scalable, as you need one ethernet port on the router for every VLAN.
2. Trunk-based inter-VLAN routing: a second method of providing routing and connectivity for multiple VLANs is through the use of an 802.1Q trunk between one or more switches and a single router interface. This method is also known as router-on-a-stick inter-VLAN routing. In this method, the physical router interface is divided into multiple subinterfaces that provide logical pathways to all VLANs connected. The downside is that a router is sacrificed just for routing between VLANs.
3. Layer 3 switching: read about it here.

Exercise 1: Configuring VLANs and Trunking (6.2.2.5)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Scenario

In this exercise, you will create VLANs on both switches in the topology, assign VLANs to switch access ports, verify that VLANs are working as expected, and then create a VLAN trunk between the two switches to allow hosts in the same VLAN to communicate through the trunk, regardless of which switch the host is actually attached to.

A. Build the Network and Configure Basic Device Settings using Cisco Packet Tracer

Step 1: Cable the network as shown in the topology.

Step 2: Configure basic settings for each switch.

a. Console into the switch and enter global configuration mode.

b. Copy the following basic configuration and paste it to the running-configuration on the switch.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
logging synchronous
login
exit
```

c. Configure the host name as shown in the topology.

d. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.

e. Administratively deactivate all unused ports on the switch.

f. Copy the running configuration to the startup configuration.

Step 3: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 4: Test connectivity.

Verify that the PC hosts can ping one another.

Can PC-A ping PC-B? Yes

Can PC-A ping PC-C? No

Can PC-A ping S1? No

Can PC-B ping PC-C? No

Can PC-B ping S2? No

Can PC-C ping S2? No

Can S1 ping S2? Yes

If you answered no to any of the above questions, why were the pings unsuccessful?

They were unable to ping as the device was on another subnet. They would have to have a default gateway in order for this to work as this would allow the subnets to meet.

B. Create VLANs and Assign Switch Ports

Now, you will create student, faculty, and management VLANs on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings.

Step 1: Create VLANs on the switches.

a. Create the VLANs on S1.

S1(config)# **vlan 10**
S1(config-vlan)# **name Student**
S1(config-vlan)# **vlan 20**
S1(config-vlan)# **name Faculty**
S1(config-vlan)# **vlan 99**
S1(config-vlan)# **name Management**
S1(config-vlan)# **end**

b. Create the same VLANs on S2.

c. Issue the **show vlan** command to view the list of VLANs on S1.

S1# **show vlan**

```
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
10   Student                           active
20   Faculty                           active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
```

1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
20 enet 100020 1500 - - - - - 0 0
99 enet 100099 1500 - - - - - 0 0

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs

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

What is the default VLAN? VLAN 1

What ports are assigned to the default VLAN?

All of the switch ports by default.

Step 2: Assign VLANs to the correct switch interfaces.

a. Assign VLANs to the interfaces on S1.

1) Assign PC-A to the Student VLAN.

S1(config)# **interface f0/6**
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan 10**

2) Move the switch IP address VLAN 99.

S1(config)# **interface vlan 1**
S1(config-if)# **no ip address**

S1(config-if)# **interface vlan 99**

S1(config-if)# **ip address 192.168.1.11 255.255.255.0**

S1(config-if)# **end**

b. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

S1# **show vlan brief**

```
VLAN Name                        Status    Ports
---- ------------------------------ --------- -------------------------------
1    default                     active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, 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
10   Student                     active    Fa0/6
20   Faculty                     active
99   Management                     active
1002 fddi-default                act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default             act/unsup
1005 trnet-default               act/unsup
```

c. Issue the **show ip interface brief** command.

What is the status of VLAN 99? Why?

The status is up/down as it has no active port.

d. Use the Topology to assign VLANs to the appropriate ports on S2.

e. Remove the IP address for VLAN 1 on S2.

f. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.

g. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

S2# **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
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24, Gi0/1, Gi0/2
10 Student active Fa0/11
20 Faculty active Fa0/18
99 Management active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

Is PC-A able to ping PC-B? Why?

No, as F0/1 is not assigned to VLAN 10 so the traffic signals won't meet.

Is S1 able to ping S2? Why?

No, as the IP addresses for the switches are in VLAN 99 and similar to above VLAN 99 don't intersect with F0/1.

C. Maintain VLAN Port Assignments and the VLAN Database

Here, you will change VLAN assignments to ports and remove VLANs from the VLAN database.

Step 1: Assign a VLAN to multiple interfaces.

a. On S1, assign interfaces F0/11 – 24 to VLAN 10.

S1(config)# **interface range f0/11-24**
S1(config-if-range)# **switchport mode access**
S1(config-if-range)# **switchport access vlan 10**
S1(config-if-range)# **end**

b. Issue the **show vlan brief** command to verify VLAN assignments.

c. Reassign F0/11 and F0/21 to VLAN 20.

d. Verify that VLAN assignments are correct.

Step 2: Remove a VLAN assignment from an interface.

a. Use the **no switchport access vlan** command to remove the VLAN 10 assignment to F0/24.

S1(config)# **interface f0/24**

S1(config-if)# **no switchport access vlan**

S1(config-if)# **end**

b. Verify that the VLAN change was made.

Which VLAN is F0/24 now associated with?

VLAN 1

Step 3: Remove a VLAN ID from the VLAN database.

a. Add VLAN 30 to interface F0/24 without issuing the VLAN command.

S1(config)# **interface f0/24**

S1(config-if)# **switchport access vlan 30**

% Access VLAN does not exist. Creating vlan 30

Note: Current switch technology no longer requires that the **vlan** command be issued to add a VLAN to the database. By assigning an unknown VLAN to a port, the VLAN adds to the VLAN database.

b. Verify that the new VLAN is displayed in the VLAN table.

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, Gi0/1, Gi0/2
10   Student                           active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/22, Fa0/23
20   Faculty                           active    Fa0/11, Fa0/21
30   VLAN0030                          active    Fa0/24
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

What is the default name of VLAN 30?

VLAN0030

c. Use the **no vlan 30** command to remove VLAN 30 from the VLAN database.

S1(config)# **no vlan 30**

S1(config)# **end**

d. Issue the **show vlan brief** command. F0/24 was assigned to VLAN 30.

After deleting VLAN 30, what VLAN is port F0/24 assigned to? What happens to the traffic destined to the host attached to F0/24?

Port F0/24 does not have a VLAN so the port will not bring in any traffic.

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

e. Issue the **no switchport access vlan** command on interface F0/24.

f. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24. To which VLAN is F0/24 assigned?

VLAN 1

Note: Before removing a VLAN from the database, it is recommended that you reassign all the ports assigned to that VLAN.

Why should you reassign a port to another VLAN before removing the VLAN from the VLAN database?

You should reassign a port to another VLAN as the interfaces assigned to a VLAN which are later removed are unable to be used until they get another VLAN.

D. Configure an 802.1Q Trunk Between the Switches

In this part, you will configure interface F0/1 to use the Dynamic Trunking Protocol (DTP) to allow it to negotiate the trunk mode. After this has been accomplished and verified, you will disable DTP on interface F0/1 and manually configure it as a trunk.

Step 1: Use DTP to initiate trunking on F0/1.

The default DTP mode of a 2960 switch port is dynamic auto. This allows the interface to convert the link to a trunk if the neighboring interface is set to trunk or dynamic desirable mode.

a. Set F0/1 on S1 to negotiate trunk mode.

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode dynamic desirable**

*Mar 1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

*Mar 1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

S1(config-if)#

*Mar 1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1(config-if)#

*Mar 1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

*Mar 1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

You should also receive link status messages on S2.

S2#

*Mar 1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

S2#

*Mar 1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S2#

*Mar 1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

b. Issue the **show vlan brief** command on S1 and S2. Interface F0/1 is no longer assigned to VLAN 1. Trunked interfaces are not listed in the VLAN table.

S1# **show vlan brief**

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

c. Issue the **show interfaces trunk** command to view trunked interfaces. Notice that the mode on S1 is set to desirable, and the mode on S2 is set to auto.

S1# **show interfaces trunk**

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

S2# **show interfaces trunk**

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

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,99

Note: By default, all VLANs are allowed on a trunk. The **switchport trunk** command allows you to control what VLANs have access to the trunk. For this lab, keep the default settings which allows all VLANs to traverse F0/1.

d. Verify that VLAN traffic is traveling over trunk interface F0/1.

Can S1 ping S2? Yes

Can PC-A ping PC-B? Yes

Can PC-A ping PC-C? No

Can PC-B ping PC-C? No

Can PC-A ping S1? No

Can PC-B ping S2? No

Can PC-C ping S2? No

If you answered no to any of the above questions, explain below.

It may not ping as they are within a different VLAN. As these switches are within different VLANs than the PCs, the pings are not successful.

Step 2: Manually configure trunk interface F0/1.

The **switchport mode trunk** command is used to manually configure a port as a trunk. This command should be issued on both ends of the link.

a. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode trunk**

b. Issue the **show interfaces trunk** command to view the trunk mode. Notice that the mode changed from **desirable** to **on**.

S2# **show interfaces trunk**

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

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Why might you want to manually configure an interface to trunk mode instead of using DTP?

This might be helpful as not all equipment uses DTP. If you use switchport mode trunk then this will allow the port to become a trunk without relying on equipment.

E. Delete the VLAN Database

Lastly, you will delete the VLAN Database from the switch. It is necessary to do this when initializing a switch back to its default settings.

Step 1: Determine if the VLAN database exists.

Issue the **show flash** command to determine if a **vlan.dat** file exists in flash.

S1# **show flash**

Directory of flash:/

```
2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
6  -rwx         736   Mar 1 1993 00:19:41 +00:00  vlan.dat
```

32514048 bytes total (20858880 bytes free)

Note: If there is a **vlan.dat** file located in flash, then the VLAN database does not contain its default settings.

Step 2: Delete the VLAN database.

a. Issue the **delete vlan.dat** command to delete the vlan.dat file from flash and reset the VLAN database back to its default settings. You will be prompted twice to confirm that you want to delete the vlan.dat file. Press Enter both times.

S1# delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

S1#

b. Issue the **show flash** command to verify that the vlan.dat file has been deleted.

S1# **show flash**

Directory of flash:/

2 -rwx 1285 Mar 1 1993 00:01:24 +00:00 config.text
3 -rwx 43032 Mar 1 1993 00:01:24 +00:00 multiple-fs
4 -rwx 5 Mar 1 1993 00:01:24 +00:00 private-config.text
5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin

32514048 bytes total (20859904 bytes free)

To initialize a switch back to its default settings, what other commands are needed?

You will need to erase startup-config, reload, and delete vlan.dat.

Reflection

1. What is needed to allow hosts on VLAN 10 to communicate to hosts on VLAN 20?

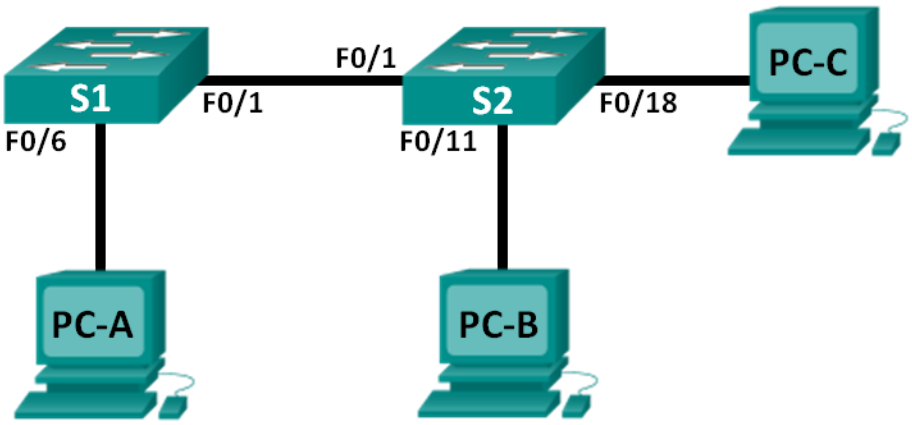
   Layer 3 routing needs to route traffic between VLANs.

2. What are some primary benefits that an organization can receive through effective use of VLANs?

   Within VLAN you have more efficiency within cost, better security, better performance, etc. The list goes on although these are the main components that may have it stand out.

Exercise 2: Troubleshooting VLAN Configurations 6.2.3.9

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
F0/1	802.1Q Trunk	N/A
F0/6-12	VLAN 10 – Students	192.168.10.0/24
F0/13-18	VLAN 20 – Faculty	192.168.20.0/24
F0/19-24	VLAN 30 – Guest	192.168.30.0/24

Scenario

In this exercise, a school has decided to implement VLANs in order to separate traffic from different end users. The school is using 802.1Q trunking to facilitate VLAN communication between switches.

The S1 and S2 switches have been configured with VLAN and trunking information. Several errors in the configuration have resulted in connectivity issues. You have been asked to troubleshoot and correct the configuration errors and document your work.

A. Build the Network and Configure Basic Device Settings using Cisco Packet Tracer

In the first part, you will set up the network topology and configure the switches with some basic settings, such as passwords and IP addresses. Preset VLAN-related configurations, which contain errors, are provided for you for the initial switch configurations. You will also configure the IP settings for the PCs in the topology.

Step 1: Cable the network as shown in the topology.

Step 2: Configure PC hosts.

Step 3: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the IP address according to the Addressing Table.

c. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.

d. Assign **class** as the privileged EXEC password.

e. Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 4: Load switch configurations.

The configurations for the switches S1 and S2 are provided for you. There are errors within these configurations, and it is your job to determine the incorrect configurations and correct them.

Switch S1 Configuration:

```
hostname S1
vlan 10
 name Students
vlan 2
name Faculty
vlan 30
 name Guest
interface range f0/1-24
 switchport mode access
 shutdown
interface range f0/7-12
 switchport access vlan 10
interface range f0/13-18
 switchport access vlan 2
interface range f0/19-24
 switchport access vlan 30
end
```

Switch S2 Configuration:

```
hostname S2
vlan 10
 name Students
vlan 20
 name Faculty
vlan 30
 name Guest
interface f0/1
 switchport mode trunk
 switchport trunk allowed vlan 1,10,2,30
interface range f0/2-24
 switchport mode access
 shutdown
interface range f0/13-18
 switchport access vlan 20
interface range f0/19-24
 switchport access vlan 30
 shutdown
end
```

Step 5: Copy the running configuration to the startup configuration.

B. Troubleshoot VLAN 10

Next, you must examine VLAN 10 on S1 and S2 to determine if it is configured correctly. You will troubleshoot the scenario until connectivity is established.

Step 1: Troubleshoot VLAN 10 on S1.

a. Can PC-A ping PC-B? No

b. After verifying that PC-A was configured correctly, examine the S1 switch to find possible configuration errors by viewing a summary of the VLAN information. Enter the **show vlan brief** command.

c. Are there any problems with the VLAN configuration?

Yes as the port for PC-A does not have the proper VLAN. As the port for F0/1 is not assigned to VLAN 1 it is not the trunk port.

d. Examine the switch for trunk configurations using the **show interfaces trunk** and the **show interfaces f0/1 switchport** commands.

e. Are there any problems with the trunking configuration?

Yes as no trunk ports exist and F0/1 is an access port rather than a trunk port.

f. Examine the running configuration of the switch to find possible configuration errors.

Are there any problems with the current configuration?

Yes F0/1-5 are all access ports and all ports are shut down.

g. Correct the errors found regarding F0/1 and VLAN 10 on S1. Record the commands used in the space below.

S1(config)# **interface f0/1**

S1(config-if)# **no shutdown**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **interface f0/6**

S1(config-if)# **no shutdown**

S1(config-if)# **switchport access vlan 10**

h. Verify the commands had the desired effects by issuing the appropriate **show** commands.

i. Can PC-A ping PC-B? No

Step 2: Troubleshoot VLAN 10 on S2.

a. Using the previous commands, examine the S2 switch to find possible configuration errors.

Are there any problems with the current configuration?

Yes as no ports are assigned to VLAN 10, also, F0/1 and F0/11 are shut down.

b. Correct the errors found regarding interfaces and VLAN 10 on S2. Record the commands below.

S2(config)# **interface range f0/6-12**

S2(config-if-range)# **switchport access vlan 10**

S2(config-if-range)# **interface f0/11**

S2(config-if)# **no shutdown**

c. Can PC-A ping PC-B? Yes

C. Troubleshoot VLAN 20

Lastly, you must examine VLAN 20 on S1 and S2 to determine if it is configured correctly. To verify functionality, you will reassign PC-A into VLAN 20, and then troubleshoot the scenario until connectivity is established.

Step 1: Assign PC-A to VLAN 20.

a. On PC-A, change the IP address to 192.168.20.2/24 with a default gateway of 192.168.20.1.

b. On S1, assign the port for PC-A to VLAN 20. Write the commands needed to complete the configuration.

S1(config)# **interface f0/6**

S1(config-if)# **switchport access vlan 20**

c. Verify that the port for PC-A has been assigned to VLAN 20.

d. Can PC-A ping PC-C? No

Step 2: Troubleshoot VLAN 20 on S1.

a. Using the previous commands, examine the S1 switch to find possible configuration errors.

Are there any problems with the current configuration?

Yes as VLAN 2 is made rather than VLAN 20 and that is where the ports are assigned to.

b. Correct the errors found regarding VLAN 20.

c. Can PC-A ping PC-C? No

Step 3: Troubleshoot VLAN 20 on S2.

a. Using the previous commands, examine the S2 switch to find possible configuration errors.

Are there any problems with the current configuration?

Yes as the trunked interface interacts with VLAN 2 rather than 20 and port F0/18 is closed.

b. Correct the errors found regarding VLAN 20. Record the commands used below.

S2(config)# **interface f0/18**

S2(config-if)# **no shutdown**

S2(config)# **interface f0/1**

S2(config-if)# **switchport trunk allowed vlan remove 2**

S2(config-if)# **switchport trunk allowed vlan add 20**

c. Can PC-A ping PC-C? Yes

Reflection

1. Why is a correctly configured trunk port critical in a multi-VLAN environment?

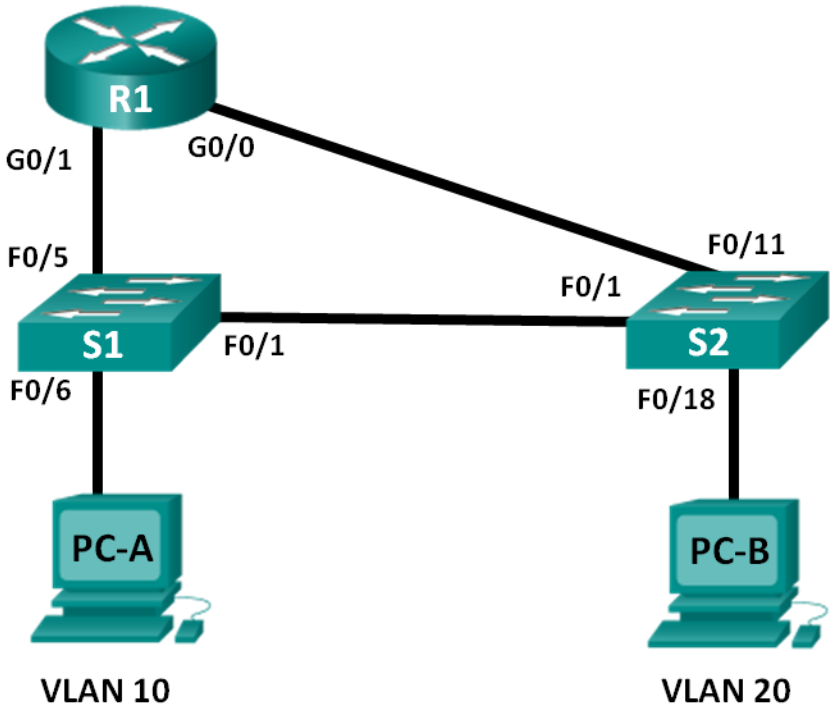
An 802.1Q trunk port allows the transmission of multiple VLANs on one link. Because of this error it may prevent VLANs from communicating across switches.

2. Why would a network administrator limit traffic for specific VLANs on a trunk port?

It is in order to keep away VLAN traffic which is not wanted.

Exercise 3: Configuring Per-Interface Inter-VLAN Routing (6.3.2.4)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	192.168.10.1	255.255.255.0	N/A
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Scenario

In this exercise, you will set up one router with two switches attached via the router Gigabit Ethernet interfaces. Two separate VLANs will be configured on the switches, and you will set up routing between the VLANs.

Note: This exercise provides minimal assistance with the actual commands necessary to configure the router and switches. The required switch VLAN configuration commands are provided in Appendix A of this lab. Test your knowledge by trying to configure the devices without referring to the appendix.

A. Build the Network and Configure Basic Device Settings

In the first part, you will set up the network topology and clear any configurations, if necessary.

Step 1: Cable the network as shown in the topology.

Step 2: Configure basic settings for R1.

a. Console into R1 and enter global configuration mode.

b. Copy the following basic configuration and paste it to the running-configuration on R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. Configure addressing on G0/0 and G0/1 and enable both interfaces.

d. Copy the running configuration to the startup configuration.

Step 3: Configure basic settings on both switches.

a. Console into the switch and enter global configuration mode.

b. Copy the following basic configuration and paste it to running-configuration on the switch.

```
no ip domain-lookup
```

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

Line con 0

password cisco

login

logging synchronous

line vty 0 15

password cisco

login

exit

c. Configure the host name as shown in the topology.

d. Copy the running configuration to the startup configuration.

Step 4: Configure basic settings on PC-A and PC-B.

Configure PC-A and PC-B with IP addresses and a default gateway address according to the Addressing Table.

B. Configure Switches with VLANs and Trunking

Second, you will configure the switches with VLANs and trunking.

Step 1: Configure VLANs on S1.

a. On S1, create VLAN 10. Assign **Student** as the VLAN name.

b. Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.

c. Configure F0/1 as a trunk port.

d. Assign ports F0/5 and F0/6 to VLAN 10 and configure both F0/5 and F0/6 as access ports.

e. Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.

f. Configure the default gateway according to the Addressing Table.

Step 2: Configure VLANs on S2.

a. On S2, create VLAN 10. Assign **Student** as the VLAN name.

b. Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.

c. Configure F0/1 as a trunk port.

d. Assign ports F0/11 and F0/18 to VLAN 20 and configure both F0/11 and F0/18 as access ports.

e. Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.

f. Configure the default gateway according to the Addressing Table.

C. Verify Trunking, VLANs, Routing, and Connectivity

Step 1: Verify the R1 routing table.

a. On R1, issue the **show ip route** command. What routes are listed on R1?

The 192.168.10.0/24 and 192.168.20.0/24

b. On both S1 and S2, issue the **show interface trunk** command. Is the F0/1 port on both switches set to trunk?

Yes

c. Issue a show vlan brief command on both S1 and S2. Verify that VLANs 10 and 20 are active and that the proper ports on the switches are in the correct VLANs. Why is F0/1 not listed in any of the active VLANs?

It is because it is a trunk port without a VLAN.

d. Ping from PC-A in VLAN 10 to PC-B in VLAN 20. If Inter-VLAN routing is functioning correctly, the pings between the 192.168.10.0 network and the 192.168.20.0 should be successful.

e. Verify connectivity between devices. You should be able to ping between all devices. Troubleshoot if you are not successful.

Reflection

What is an advantage of using legacy inter-VLAN routing?

You may configure both the router and switches extremely easily.

Appendix A: Configuration Commands

Switch S1

S1(config)**# vlan 10**

S1(config-vlan)**# name Student**

S1(config-vlan)**# exit**

S1(config)**# vlan 20**

S1(config-vlan)**# name Faculty-Admin**

S1(config-vlan)**# exit**

S1(config)**# interface f0/1**

S1(config-if)**# switchport mode trunk**

S1(config-if)**# interface range f0/5 – 6**

S1(config-if-range)**# switchport mode access**

S1(config-if-range)# **switchport access vlan 10**

S1(config-if-range)# **interface vlan 10**

S1(config-if)# **ip address 192.168.10.11 255.255.255.0**

S1(config-if)# **no shut**

S1(config-if)# **exit**

S1(config)# **ip default-gateway 192.168.10.1**

Switch S2

S2(config)# **vlan 10**

S2(config-vlan)# **name Student**

S2(config-vlan)# **exit**

S2(config)# **vlan 20**

S2(config-vlan)# **name Faculty-Admin**

S2(config-vlan)# **exit**

S2(config)# **interface f0/1**

S2(config-if)# **switchport mode trunk**

S2(config-if)# **interface f0/11**

S2(config-if)# **switchport mode access**

S2(config-if)# **switchport access vlan 20**

S2(config-if)# **interface f0/18**

S2(config-if)# **switchport mode access**

S2(config-if)# **switchport access vlan 20**

S2(config-if-range)# **interface vlan 10**

S2(config-if)#**ip address 192.168.10.12 255.255.255.0**

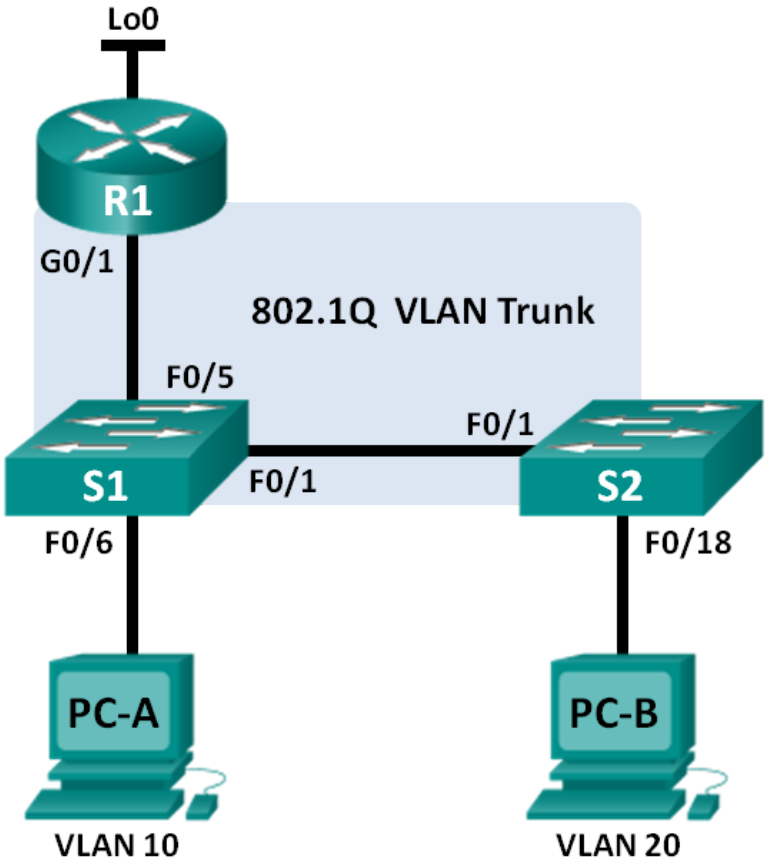
S2(config-if)# **no shut**

S2(config-if)# **exit**

S2(config)# **ip default-gateway 192.168.10.1**

Exercise 4: Configuring 802.1Q Trunk-Based Inter-VLAN Routing (6.3.3.7)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
S1 F0/1	802.1Q Trunk	N/A
S2 F0/1	802.1Q Trunk	N/A
S1 F0/5	802.1Q Trunk	N/A
S1 F0/6	VLAN 10 – Students	192.168.10.0/24
S2 F0/18	VLAN 20 – Faculty	192.168.20.0/24

Scenario

In this exercise, you will configure trunk-based inter-VLAN routing and verify connectivity to hosts on different VLANs as well as with a loopback on the router.

Note: This exercise provides minimal assistance with the actual commands necessary to configure trunk-based inter-VLAN routing. However, the required configuration commands are provided in Appendix A of this lab. Test your knowledge by trying to configure the devices without referring to the appendix.

A. Build the Network and Configure Basic Device Settings

In the first part, you will set up the network topology and configure basic settings on the PC hosts, switches, and router.

Step 1: Cable the network as shown in the topology.

Step 2: Configure PC hosts.

Step 3: Configure basic settings for each switch.

a. Console into the switch and enter global configuration mode.

a. Copy the following basic configuration and paste it to the running-configuration on the switch.

no ip domain-lookup

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

line con 0

password cisco

login

logging synchronous

line vty 0 15

password cisco

login

exit

b. Configure the device name as shown in the topology.

c. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.

d. Configure the default gateway on the switch.

e. Administratively deactivate all unused ports on the switch.

f. Copy the running configuration to the startup configuration.

Step 4: Configure basic settings for the router.

a. Console into the router and enter global configuration mode.

g. Copy the following basic configuration and paste it to the running-configuration on the router.

no ip domain-lookup

hostname R1

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

Line con 0

password cisco

login

logging synchronous

line vty 0 4

password cisco

login

h. Configure the Lo0 IP address as shown in the Address Table. Do not configure subinterfaces at this time. They will be configured in Part 3.

i. Copy the running configuration to the startup configuration.

B. Configure Switches with VLANs and Trunking

In the second part, you will configure the switches with VLANs and trunking.

Step 1: Configure VLANs on S1.

a. On S1, configure the VLANs and names listed in the Switch Port Assignment Specifications table. Write the commands you used in the space provided.

S1(config)# vlan 10

S1(config-vlan)# name Students

S1(config-vlan)# vlan 20

S1(config-vlan)# name Faculty

S1(config-vlan)# exit

j. On S1, configure the interface connected to R1 as a trunk. Also configure the interface connected to S2 as a trunk. Write the commands you used in the space provided.

S1(config)# interface f0/5

S1(config-if)# switchport mode trunk

S1(config-if)# interface f0/1

S1(config-if)# switchport mode trunk

k. On S1, assign the access port for PC-A to VLAN 10. Write the commands you used in the space provided.

S1(config)# interface f0/6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 10

Step 2: Configure VLANs on Switch 2.

a. On S2, configure the VLANs and names listed in the Switch Port Assignment Specifications table.

l. On S2, verify that the VLAN names and numbers match those on S1. Write the command you used in the space provided.

S2# show vlan brief

m. On S2, assign the access port for PC-B to VLAN 20.

n. On S2, configure the interface connected to S1 as a trunk.

C. Configure Trunk-Based Inter-VLAN Routing

Lastly, you will configure R1 to route to multiple VLANs by creating subinterfaces for each VLAN. This method of inter-VLAN routing is called router-on-a-stick.

Step 1: Configure a subinterface for VLAN 1.

a. Create a subinterface on R1 G0/1 for VLAN 1 using 1 as the subinterface ID. Write the command you used in the space provided.

R1(config)# interface g0/1.1

o. Configure the subinterface to operate on VLAN 1. Write the command you used in the space provided.

R1(config-subif)# encapsulation dot1Q 1

p. Configure the subinterface with the IP address from the Address Table. Write the command you used in the space provided.

R1(config-subif)# ip address 192.168.1.1 255.255.255.0

Step 2: Configure a subinterface for VLAN 10.

a. Create a subinterface on R1 G0/1 for VLAN 10 using 10 as the subinterface ID.

q. Configure the subinterface to operate on VLAN 10.

r. Configure the subinterface with the address from the Address Table.

Step 3: Configure a subinterface for VLAN 20.

a. Create a subinterface on R1 G0/1 for VLAN 20 using 20 as the subinterface ID.

s. Configure the subinterface to operate on VLAN 20.

t. Configure the subinterface with the address from the Address Table.

Step 4: Enable the G0/1 interface.

Enable the G0/1 interface. Write the commands you used in the space provided.

R1(config)# interface g0/1

R1(config-if)# no shutdown

Step 5: Verify connectivity.

Enter the command to view the routing table on R1. What networks are listed?

192.168.1.0, 192.168.10.0, 192.168.20.0, and 209.165.200.224

From PC-A, is it possible to ping the default gateway for VLAN 10? Yes

From PC-A, is it possible to ping PC-B? Yes

From PC-A, is it possible to ping Lo0? Yes

From PC-A, is it possible to ping S2? Yes

If the answer is **no** to any of these questions, troubleshoot the configurations and correct any errors.

Reflection

What are the advantages of trunk-based or router-on-a-stick inter-VLAN routing?

Router-on-a-stick inter-VLAN will allow for a one-to-many route for VLANs although the trunk-based inter-VLAN method requires one port per VLAN.

Appendix A – Configuration Commands

Switch S1

S1(config)**# vlan 10**

S1(config-vlan)**# name Students**

S1(config-vlan)**# vlan 20**

S1(config-vlan)**# name Faculty**

S1(config-vlan)**# exit**

S1(config)**# interface f0/1**

S1(config-if)**# switchport mode trunk**

S1(config-if)**# interface f0/5**

S1(config-if)**# switchport mode trunk**

S1(config-if)**# interface f0/6**

S1(config-if)**# switchport mode access**

S1(config-if)**# switchport access vlan 10**

Switch S2

S2(config)**# vlan 10**

S2(config-vlan)**# name Students**

S2(config-vlan)**# vlan 20**

S2(config-vlan)**# name Faculty**

S2(config)**# interface f0/1**

S2(config-if)**# switchport mode trunk**

S2(config-if)**# interface f0/18**

S2(config-if)**# switchport mode access**

S2(config-if)**# switchport access vlan 20**

Router R1

R1(config)**# interface g0/1.1**

R1(config-subif)**# encapsulation dot1Q 1**

R1(config-subif)**# ip address 192.168.1.1 255.255.255.0**

R1(config-subif)**# interface g0/1.10**

R1(config-subif)**# encapsulation dot1Q 10**

R1(config-subif)# **ip address 192.168.10.1 255.255.255.0**

R1(config-subif)# **interface g0/1.20**

R1(config-subif)# **encapsulation dot1Q 20**

R1(config-subif)# **ip address 192.168.20.1 255.255.255.0**

R1(config-subif)# **exit**

R1(config)# **interface g0/1**

R1(config-if)# **no shutdown**