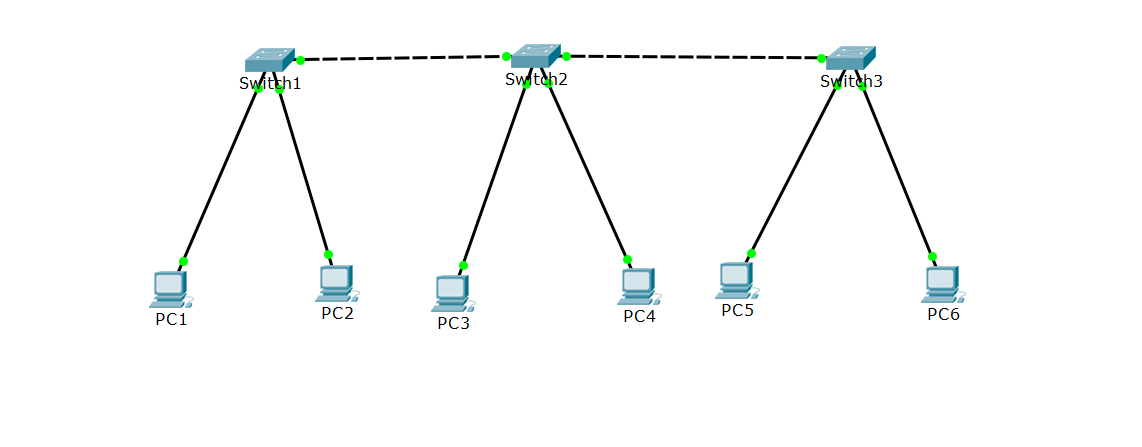
Lab 3A- Packet Tracer – Configuring VLANs, Trunking



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DEVICES** | **INTERFACE** | **IP ADDRESS** | **SUBNET** | **VLAN** |
| PC1 | NIC | 192.168.10.1 | 255.255.255.0 | 10 |
| PC2 | NIC | 192.168.20.1 | 255.255.255.0 | 20 |
| PC3 | NIC | 192.168.10.2 | 255.255.255.0 | 10 |
| PC4 | NIC | 192.168.20.2 | 255.255.255.0 | 20 |
| PC5 | NIC | 192.168.10.3 | 255.255.255.0 | 10 |
| PC6 | NIC | 192.168.20.3 | 255.255.255.0 | 20 |

1. Objectives

Part 1: Verify the Default VLAN Configuration

Part 2: Configure VLANs

Part 3: Assign VLANs to Ports

Background

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

1. PART 1: View the Default VLAN Configuration

**Step 1: Set the IP address and Subnet mask for all the 6 PCs.**

Step 2: Display the current VLANs.

On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.

Step 3: Verify connectivity between PCs on the same network.

Notice that each PC can ping the other PC that shares the same network.

* PC1 can ping PC3 and PC5
* PC2 can ping PC4 and PC6

Pings to PCs in other networks fail.

What benefit will configuring VLANs provide to the current configuration?

1. Configure VLANs
   1. Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

* VLAN 10: Faculty/Staff

**S1(conft)# vlan 10**

**S1(conft)#name Faculty/Staff**

* VLAN 20: Students

**S1(conft)# vlan 20**

**S1(conft)#name Students**

* VLAN 30: Guest(Default)

**S1(conft)# vlan 30**

**S1(conft)#name Guest(Default)**

* VLAN 40: Management&Native

**S1(conft)# vlan 40**

**S1(conft)#name Management&Native**

* 1. Verify the VLAN configuration.

Which command will only display the VLAN name, status, and associated ports on a switch?

S1#Show vlan

* 1. Create the VLANs on S2 and S3.

Using the same commands from Step 1, create and name the same VLANs on S2 and S3.

* 1. Verify the VLAN configuration.

1. Assign VLANs to Ports
   1. Assign VLANs to the active ports on S1

Assign VLANs to the following ports:

* VLAN 10: FastEthernet0/2

**S1(conft)# int f0/2**

**S1(conf-if)#Switchport mode access**

**S1(conf-if)#Switchport access vlan 10**

* VLAN 20: FastEthernet0/3

**S1(conft)# int f0/3**

**S1(conf-if)#Switchport mode access**

**S1(conf-if)#Switchport access vlan 20**

* 1. Assign VLANs to the active ports on S2

Assign VLANs to the following ports:

* VLAN 10: FastEthernet0/3
* VLAN 20: FastEthernet0/4
  1. Assign VLANs to the active ports on S3

Assign VLANs to the following ports:

* VLAN 10: FastEthernet0/2
* VLAN 20: FastEthernet0/3

Step 4: Verify loss of connectivity.

Previously, PCs that shared the same network could ping each other successfully. Try pinging between PC1 and PC3. Although the access ports are assigned to the appropriate VLANs, were the pings successful? Why?

What could be done to resolve this issue?

The pings weren’t successful and the reason is because there is no way for the switches to communicate what is being said on vlan 10 to the other switches.

Step 5: Verify loss of connectivity between PCs on the same network.

Although **PC1** and **PC3** are on the same network, they cannot ping one another. This is because the ports connecting the switches are assigned to VLAN 1 by default. In order to provide connectivity between the PCs on the same network and VLAN, trunks must be configured.

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

1. Configure Trunks
   1. Configure trunking on S1 for the following interface

* Interface F0/1

**S1(conft)# int f0/1**

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

Step 2: Configure trunking on S2 for the following interfaces

* Interface F0/1
* Interface F0/2

Step 3: Configure trunking on S3 for the following interface

* Interface F0/1

Step 4: Verify trunking is enabled on S1, S2 and S3.

On **S1, S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully trunked.

Which active VLANs are allowed to across the trunk?

All vlans.

**Step 5: Check the connectivity**

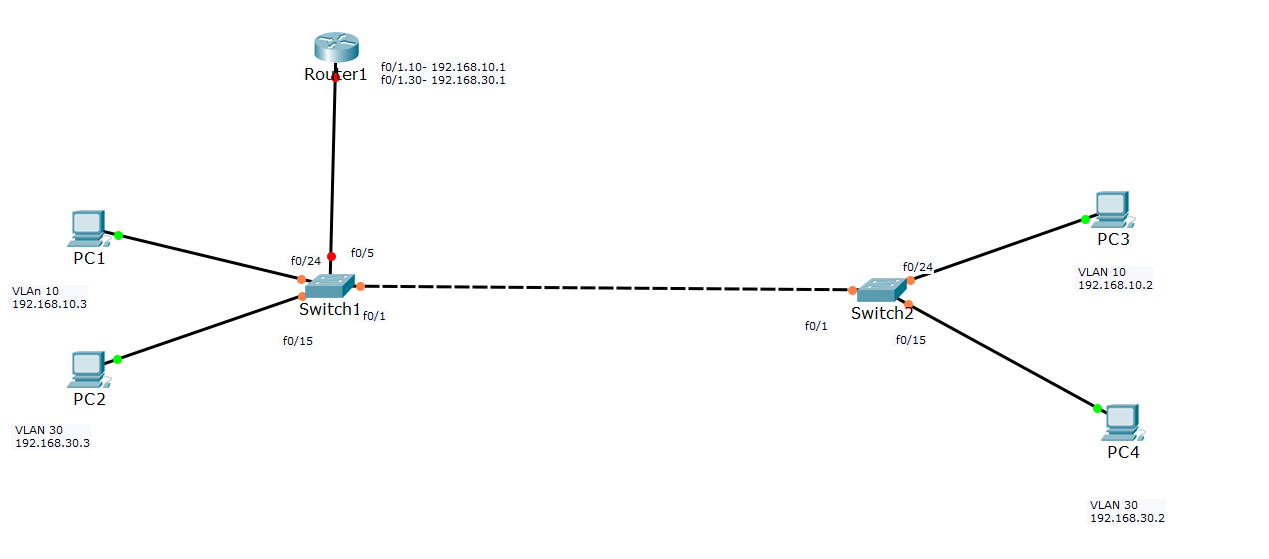
Ping from PC1 to PC3 and PC5. The ping should be successful. Also, try to ping from PC2 to PC4 and PC6.

Suggested Scoring Rubric

|  |  |  |  |
| --- | --- | --- | --- |
| Activity Section | Possible Points | | Earned Points |
| Part 1: Verify the Default VLAN Configuration | | **5** |  |
| Part 2: Configure VLANs | | **15** |  |
| Part 3: Assign VLANs to Ports | | **12.5** |  |
| Part 4: Verify VLANs | | **5** |  |
| Part 5: Configure Trunks | | **12.5** |  |
| **Total Score** | **50** | |  |

**Lab 3B – Router-on-a-stick Inter-VLAN Routing**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| PC1 | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC2 | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |
| PC3 | NIC | 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |
| PC4 | NIC | 192.168.30.2 | 255.255.255.0 | 192.168.30.1 |
| R1 | F0/1.10 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | F0/1.30 | 192.168.30.1 | 255.255.255.0 | N/A |



**TASK 1: Create VLAN 10 and 30 – 10 points**

* On S1, Create VLAN 10 and 30
* Assign ports to both the VLANs and set the ports as access ports. Refer the topology given.
* Using the topology given above, configure the trunk port.
* Repeat the above steps for S2.

**TASK 2: Check the connectivity – 10 points**

* Try to ping from PC1 to PC3 and PC1 to PC4.
* Also, try to ping PC2 to PC4

At this point, you should be able to ping between the hosts in the same network. But, when you try to ping the hosts in different network, the pings will fail. This is because, for inter-VALN routing, a layer 3 device is required. In our lab, that layer 3 device is the router which is not yet configured. Hence the ping between different networks (that is from VLAN 10 to VLAN 30 or vice-versa) fails.

**TASK 3: Router configuration – 10 points**

* Refer the table given above and create two sub-interfaces on R1 and activate them.
* Set the encapsulation type to dot1q and assign proper VLAN to that interface
* Assign the IP addresses as given in the table.

**TASK 4: S1 configuration- 10points**

* S1 is connected to R1 via interface f0/5. So configure that port on S1 as a trunk port by executing the correct command.

**TASK 5: Test the connectivity – 10 points**

* Ping between PC1 and PC4
* Ping between PC2 and PC3

**Lab 3C – Configuring Per-Interface Inter-VLAN Routing**

Diagram

Description automatically generated

**Objectives**

#### Part 1: Build the Network and Configure Basic Device Settings Part 2: Configure Switches with VLANs and Trunking

**Part 3: Verify Trunking, VLANs, Routing, and Connectivity**

**Background / Scenario**

Legacy inter-VLAN routing is seldom used in today’s networks; however, it is helpful to configure and understand this type of routing before moving on to router-on-a-stick (trunk-based) inter-VLAN routing

**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 |

### **Part 1: Configure Switches with VLANs and Trunking**

In Part 1, you will configure the switches with VLANs and Trunking.

### Step 1: Configure VLANs on S1.

1. On S1, create VLAN 10. Assign **Student** as the VLAN name.
2. Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.
3. Configure F0/1 as a trunk port.
4. Assign ports F0/5 and F0/6 to VLAN 10 and configure both F0/5 and F0/6 as access ports.
5. Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.
6. Configure the default gateway according to the Addressing Table.

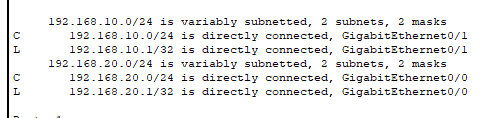
### Step 2: Configure VLANs on S2.

1. On S2, create VLAN 10. Assign **Student** as the VLAN name.
2. Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.
3. Configure F0/1 as a trunk port.
4. Assign ports F0/11 and F0/18 to VLAN 20 and configure both F0/11 and F0/18 as access ports.
5. Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.
6. Configure the default gateway according to the Addressing Table.

# **Part 2: Verify Trunking, VLANs, Routing, and Connectivity**

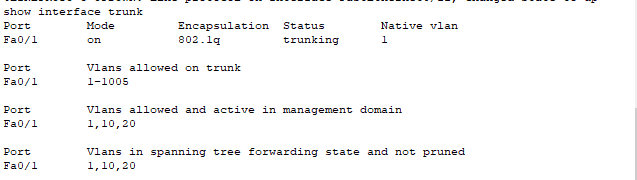
### Step 1: Verify the R1 routing table.

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

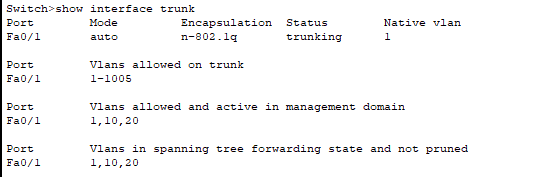


1. On both S1 and S2, issue the **show interface trunk** command. Is the F0/1 port on both switches set to trunk?

S2



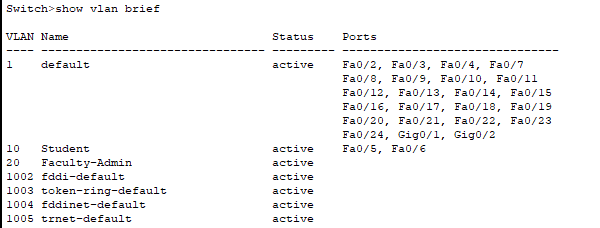
S1



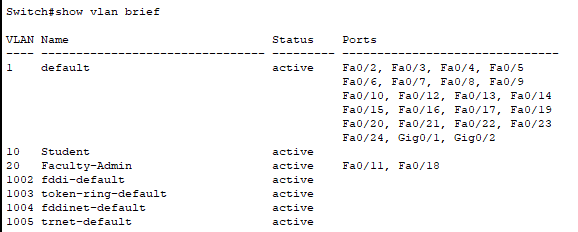
Yes

1. 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?

S1

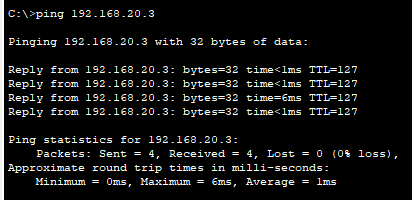


S2



Because FA0/1 is a trunk for both switches.

1. 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.



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

