**Laboratory 7 – VLAN configuration**

Student name: Phan Phương Duy Student ID: ITITIU16010

***Lab 7.1: VLAN Configuration***

**Topology Diagram**

**PC1**

**S1**



**PC3**

**PC2**

**PC4**

**PC5**

**PC6**

**S2**

Fa0/11

Fa0/18

Fa0/6

Fa0/6

Fa0/18

Fa0/11

Fa0/1

Fa0/1

**Addressing Table**

**x = 0**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| S1 | VLAN 1 | 172.0.9.12 | 255.255.255.0 | N/A |
| S2 | VLAN 1 | 172.0.9.13 | 255.255.255.0 | N/A |
| PC1 | NIC | 172.0.1.21 | 255.255.255.0 | 172.0. 1.1 |
| PC2 | NIC | 172.0.2.22 | 255.255.255.0 | 172.0. 2.1 |
| PC3 | NIC | 172.0.3.23 | 255.255.255.0 | 172.0. 3.1 |
| PC4 | NIC | 172.0.1.24 | 255.255.255.0 | 172.0. 1.1 |
| PC5 | NIC | 172.0.2.25 | 255.255.255.0 | 172.0. 2.1 |
| PC6 | NIC | 172.0.3.26 | 255.255.255.0 | 172.0. 3.1 |

Initial Port Assignments (Switches 1 and 2)

|  |  |  |
| --- | --- | --- |
| **Ports** | **Assignment** | **Network** |
| Fa0/1 – 0/5 | 802.1q Trunks (Native VLAN 1) | 172.0.9.0 /24 |
| Fa0/6 – 0/10 | VLAN 3 – Guest (Default) | 172.0.3.0 /24 |
| Fa0/11 – 0/17 | VLAN 4 – Faculty/Staff | 172.0.1.0 /24 |
| Fa0/18 – 0/24 | VLAN 2 – Students | 172.0.2.0 /24 |

**Learning Objectives**

Upon completion of this lab, you will be able to:

* Understanding the **access mode** and **trunk mode** of a port.
* Cable a network according to the topology diagram
* Erase the startup configuration and reload a switch to the default state
* Perform basic configuration tasks on a switch
* Create VLANs
* Assign switch ports to a VLAN
* Add, move, and change ports
* Verify VLAN configuration
* Enable trunking on inter-switch connections
* Verify trunk configuration
* Save the VLAN configuration

**Task 1: Prepare the Network**

**Step 1: Cable a network that is similar to the one in the topology diagram.**

You can use any current switch in your lab as long as it has the required interfaces shown in the topology.

**Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.**

If necessary, refer to the Basic Switch Configuration lab for the procedure to clear switch configurations.

It is a good practice to disable any unused ports on the switches by putting them in shutdown. Disable all ports on the switches. For example in a switch with 24 Fast-Ethernet ports and 2 Giga-Ethernet ports:

Switch(config)#interface range fa0/1-24

Switch(config-if-range)#shutdown

Switch(config-if-range)#interface range gi0/1-2

Switch(config-if-range)#shutdown

**Task 2: Perform Basic Switch Configurations**

**Step 1: Configure the switches according to the following guidelines.**

1. Configure the switch hostname.
2. Disable DNS lookup.
3. Configure an EXEC mode password of class.
4. Configure a password of **cisco** for console connections.

**Step 2: Re-enable the user ports on S1 and S2.**

S1(config)#interface range fa0/6, fa0/11, fa0/18

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

S1(config-if-range)#no shutdown

S2(config)#interface range fa0/6, fa0/11, fa0/18

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

S2(config-if-range)#no shutdown

**Step 3: Understand the access mode of a switch port**

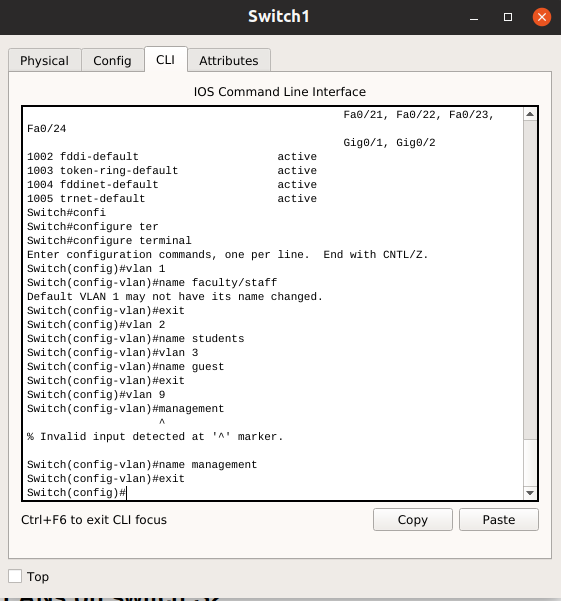
.

**Task 3: Configure the IPs and default gateways for the PCs**

**Task 4: Configure VLANs on the Switch**

**Step 1: Create VLANs on switch S1.**

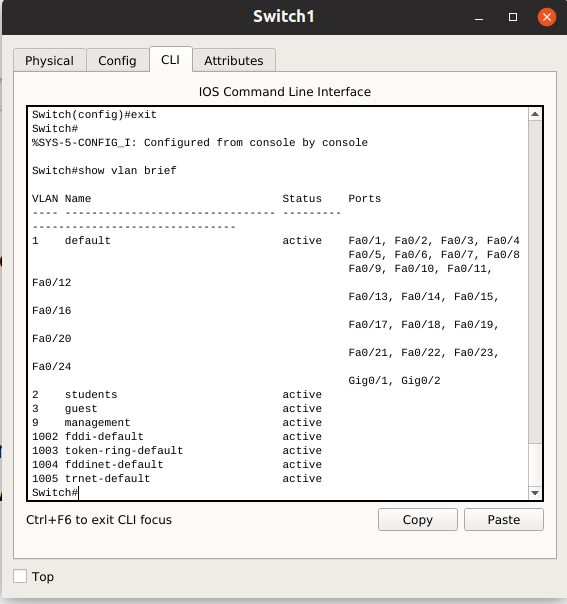
Use the vlan vlan-id command in global configuration mode to add a VLAN to switch S1. There are four VLANS configured for this lab: VLAN 1 (faculty/staff); VLAN 2 (students); VLAN 3 (guest); and VLAN 9 (management). After you create the VLAN, you will be in vlan configuration mode, where you can assign a name to the VLAN with the name vlan name command.



**Step 2: Verify that the VLANs have been created on S1.**

Use the show vlan brief command to verify that the VLANs have been created.

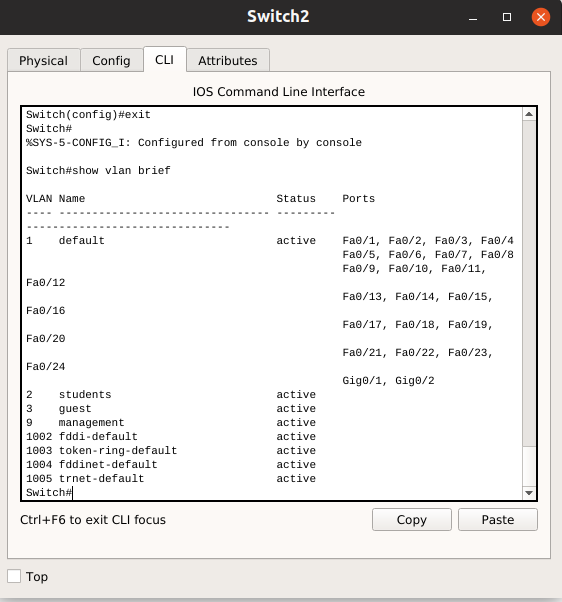
Paste your output here.



Are there VLANs you have been created ?

**Step 3: Configure and name VLANs on switch S2.**

Create and name VLANs 1, 2, 3, and 9 on S2 using the commands from Step 1. Verify the correct configuration with the show vlan brief command.



What ports are currently assigned to the four VLANs you have created?

**Step 4: Assign switch ports to VLANs on S1 and S2.**

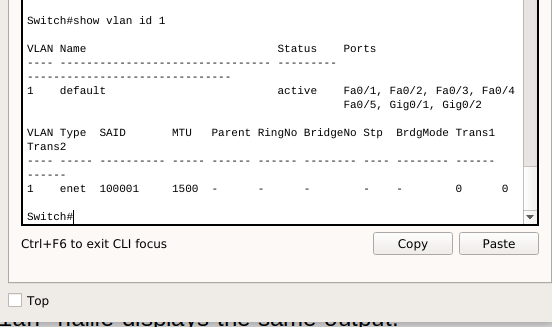
Refer to the port assignment table on page 1. Ports are assigned to VLANs in interface configuration mode, using the switchport access vlan vlan-id command. You can assign each port individually or you can use the interface range command to simplify this task. For example,

* ports fa0/6-10: vlan 3
* ports fa0/11-17: vlan 1
* ports fa0/18-24: vlan 2

Save your configuration when done.

**Step 5: Determine which ports have been added.**

Use the show vlan id vlan-number command on S1 to see which ports are assigned to VLAN 1.



Which ports are assigned to VLAN 1?

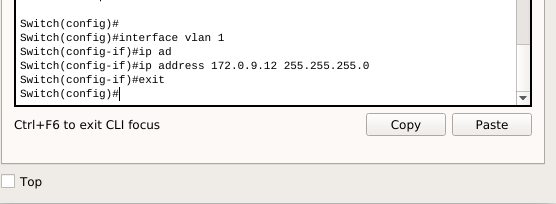
**Note**: The show vlan name vlan-name displays the same output.

You can also view VLAN assignment information using the show interfaces interface switchport command.

**Step 6: Assign the management VLAN.**

A management VLAN is any VLAN that you configure to access the management capabilities of a switch. By default, VLAN 1 serves as the management VLAN. The management VLAN is assigned an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. However, VLAN 1 is a bad choice as the management VLAN for security reason. You can assign any VLAN as management VLAN, i.e., VLAN 9 in this lab.

From interface configuration mode, use the ip address command to assign the management IP address to the switches.



Why we need a management VLAN in a network and why using VLAN as management VLAN is unsecure?

**Step 7: Configure trunking and the native VLAN for the trunking ports on all switches.**

Trunks are connections between the switches that allow the switches to exchange information for all VLANS. By default, a trunk port belongs to all VLANs, as opposed to an access port, which can only belong to a single VLAN. If the switch supports both ISL and 802.1Q VLAN encapsulation, the trunks must specify which method is being used.

A native VLAN is assigned to an 802.1Q trunk port. In the topology, the native VLAN is VLAN 9. 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). The 802.1Q trunk port places untagged traffic on the native VLAN. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. One of the IEEE 802.1Q specifications for Native VLANs is to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For the purposes of this lab, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

Use the interface range command in global configuration mode to assign port fa0/1-5 to native VLAN. For example on S1:

S1(config)# interface range fa0/1-5

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

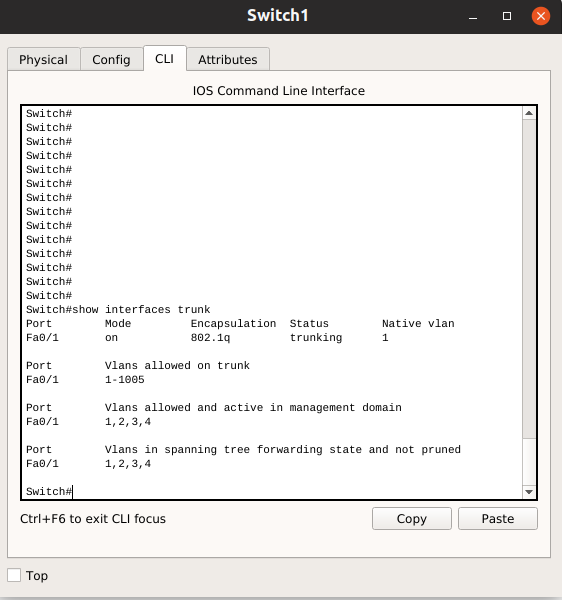
S1(config-if-range)#switchport trunk native vlan 9

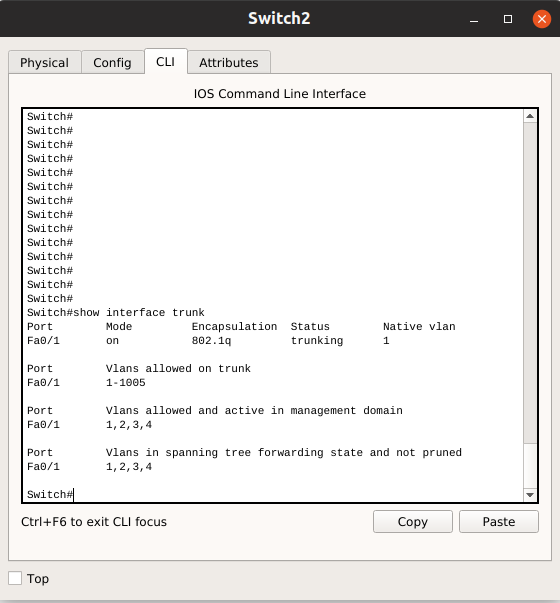
S1(config-if-range)#no shutdown

Verify that the trunks have been configured with the show interface trunk command.

S1#show interface trunk

Paste your output here.

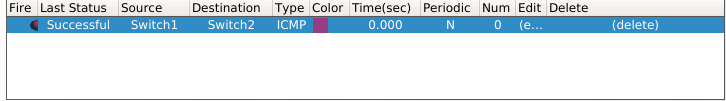




Which VLAN are allowed on trunks ?

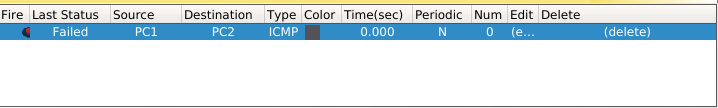
**Step 8: Verify that the switches can communicate.**

From S1, ping the management address on S2. Is the ping successful?

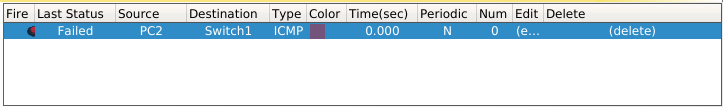


**Step 9: Ping several hosts from PC2.**

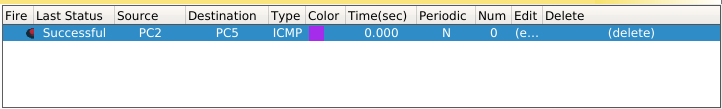
Ping from host PC2 to host PC1. Is the ping attempt successful and why?

Because PC1 and PC2 are on different VLAN

Ping from host PC2 to the switch VLAN 9 IP address 172.x.9.12. Is the ping attempt successful and why?



Ping from host PC2 to host PC5. Is the ping attempt successful and why?

The ping is successful because PC2 and PC5 are on the same VLAN

**Step 10: Move PC1 into the same VLAN as PC2.**

The port connected to PC2 (S1 Fa0/18) is assigned to VLAN 2, and the port connected to PC1 (S1 Fa0/11) is assigned to VLAN x1. Reassign the S1 Fa0/11 port to VLAN 2. You do not need to first remove a port from a VLAN to change its VLAN membership. After you reassign a port to a new VLAN by switchport access vlan 2 command, that port is automatically removed from its previous VLAN.

S1#configure terminal

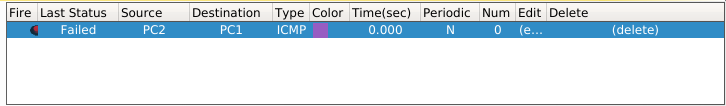
Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#interface fastethernet 0/11

S1(config-if)#switchport access vlan 2

S1(config-if)#end

Ping from host PC2 to host PC1. Is the ping attempt successful and why?



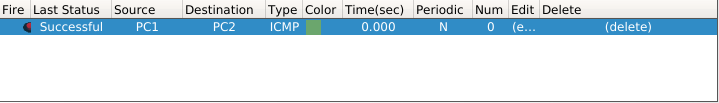
Even though the ports used by PC1 and PC2 are in the same VLAN, they are still in different

subnetworks, so they cannot communicate directly.

**Step 11: Change the IP address and network on PC1.**

Change the IP address on PC1 to 172.x.2.21. The subnet mask and default gateway can remain the same. Once again, ping from host PC2 to host PC1, using the newly assigned IP address.

Is the ping attempt successful and why?



Now PC1 and PC2 can ping each other because they are on the same VLAN and same subnet

**Step 12: Understand the trunk port mode of a switch port**

**Task 5: Document the Switch Configurations**

***Lab 7.2: Inter-VLAN Routing Configuration***

**Topology**



**Addressing Table**

**x = 0**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hostname** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| S1 | VLAN 1 | 172.0.9.11 | 255.255.255.0 | 172.0.9.1 |
| R1 | Fa 0/0 | 172.0.5.1 | 255.255.255.0 | N/A |
|  | Fa 0/1 |  |  | N/A |
| PC1 | NIC | 172.0.1.21 | 255.255.255.0 | 172.0.1.1 |
| PC2 | NIC | 172.0.2.22 | 255.255.255.0 | 172.0.2.1 |
| PC3 | NIC | 172.0.3.23 | 255.255.255.0 | 172.0.3.1 |
| Server | NIC | 172.0.5.254 | 255.255.255.0 | 172.0.5.1 |

**Port Assignments – Switch 1**

|  |  |  |
| --- | --- | --- |
| Ports | Assignment | Network |
| Fa0/1 – 0/5 | 802.1q Trunks(Native VLAN1) | 172.0.9.0/24 |
| Fa0/6 - 0/10 | VLAN 3 – Guest(default) | 172.0.3.0/24 |
| Fa0/11 - 0/17 | VLAN 4 – Faculty/Staff | 172.0.1.0/24 |
| Fa0/18 - 0/24 | VLAN 2 - Student | 172.0.2.0/24 |

**Interface Configuration Table – Router 1**

|  |  |  |
| --- | --- | --- |
| **Interface** | **Assignment** | **IP Address** |
| Fa0/1.1 | VLAN 4 | 172.0.1.1 /24 |
| Fa0/1.2 | VLAN 2 | 172.0.2.1 /24 |
| Fa0/1.3 | VLAN 3 | 172.0.3.1 /24 |

**Learning Objectives**

Upon completion of this lab, you will be able to:

* Cable a network according to the topology diagram
* Clear configurations and reload a switch and a router to the default state
* Perform basic configuration tasks on a switched LAN and router
* Configure VLANs and VLAN Trunking Protocol (VTP) on all switches
* Demonstrate and explain the impact of Layer 3 boundaries imposed by creating VLANs
* Configure a router to support 802.1q trunking on a Fast Ethernet interface
* Configure a router with subinterfaces corresponding to the configured VLANs
* Demonstrate and explain inter-VLAN routing

**Task 1: Prepare the Network**

**Step 1: Cable a network that is similar to the one in the topology diagram.**

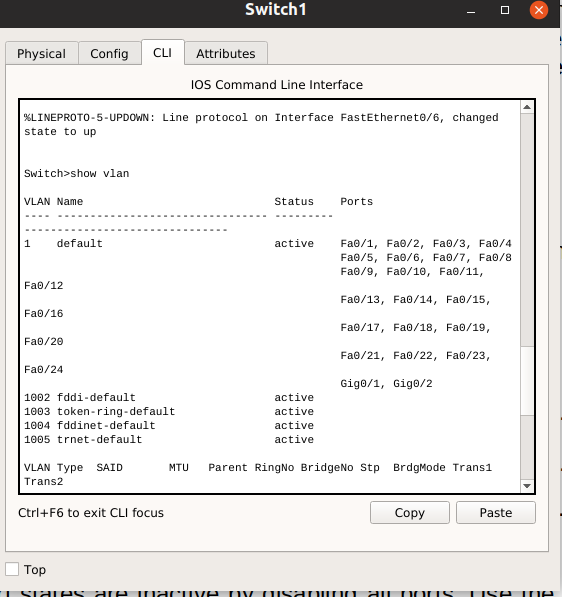
The output shown in this lab is based on 2960 switches and an 2800 router. You can use any current switches or routers in your lab as long as they have the required interfaces shown in the topology diagram. Other device types may produce different output. Note that Ethernet (10Mb) LAN interfaces on routers do not support trunking, and Cisco IOS software earlier than version 12.3 may not support trunking on Fast Ethernet router interfaces.

**Step 2: Clear any existing configurations on the switches.**

Clear NVRAM, delete the vlan.dat file, and reload the switches. Use the show vlan command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Switch#show vlan

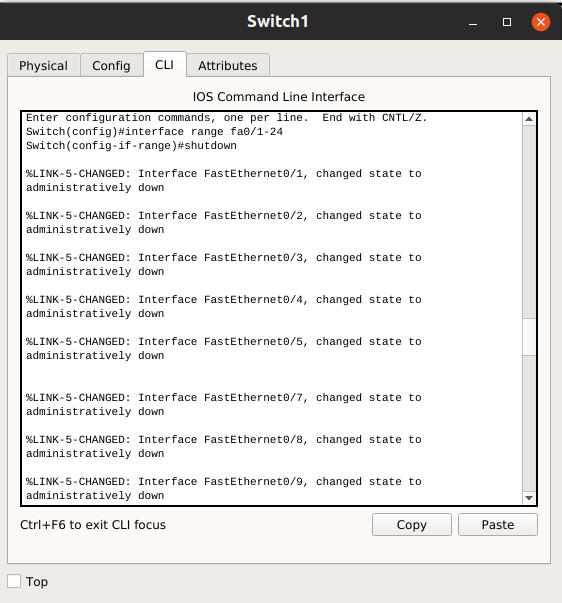
Paste your output here.



Do all ports belong to VLAN 1 ?

**Step 3: Disable all ports using the shutdown command.**

Ensure that the initial switch port states are inactive by disabling all ports. Use the interface range command to simplify this task.



**Task 2: Perform Basic Switch Configurations**

**Step 1: Configure the switch.**

Use the addressing table and the following guidelines:

* Configure the switch hostname.
* Disable DNS lookup.
* Configure an enable secret password of class.
* Configure a password of cisco for console connections.
* Configure the default gateway on each switch

**Step 2: Re-enable the active user ports on S1 in access mode.**

**Task 3: Configure the Ethernet Interfaces on the Host PCs**

Configure the Ethernet interfaces of PC1, PC2, PC3 with the IP addresses from the addressing table.

**Task 4: Configure trunk on the Switch**

**Step 2: Configure trunking ports and designate the native VLAN for the trunks.**

Configure Fa0/1 through Fa0/5 as trunking ports, and designate VLAN x9 as the native VLAN for these trunks. Use the interface range command in global configuration mode to simplify this task.

S1(config)#interface range fa0/1-5   
S1(config-if-range)#switchport mode trunk   
S1(config-if-range)#switchport trunk native vlan x9   
S1(config-if-range)#no shutdown   
S1(config-if-range)#end

**Step 3: Configure VLANs on the switch.**

Configure the following VLANS on the switch S1:

**VLAN Name**

VLAN 1 management

VLAN 4 faculty-staff

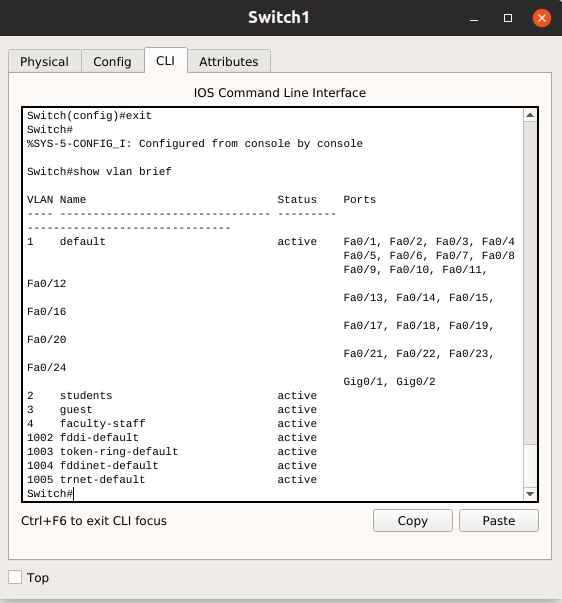
VLAN 2 students

VLAN 3 guest

**Step 4: Verify that the VLANs have been created on switch.**

Use the show vlan brief command to verify that the VLANs have been created.

Paste your output here.



Are there VLANs you have been created ?

**Step 5: Configure the management interface address on switch.**

**Step 6: Assign switch ports to VLANs on S1.**

Refer to the port assignments table at the beginning of the lab to assign ports to VLANs on S1.

**Step 7: Check connectivity between VLANs.**

Open command windows on the three hosts connected to S1. Ping from PC1 to PC2. Ping from PC2 to PC3.

Are the pings successful and why? No

**Task 5: Configure the Router and the Remote Server LAN**

**Step 1: Clear the configuration on the router and reload.**

**Step 2: Create a basic configuration on the router.**

1. Configure the router with hostname R1.
2. Disable DNS lookup.
3. Configure an EXEC mode password of cisco.
4. Configure a password of cisco for console connections.

**Step 3: Configure the trunking interface on R1.**

You have demonstrated that connectivity between VLANs requires routing at the network layer, exactly like connectivity between any two remote networks. There are a couple of options for configuring routing between VLANs.

The first is something of a brute force approach. An L3 device, either a router or a Layer 3 capable switch, is connected to a LAN switch with multiple connections--a separate connection for each VLAN that requires inter-VLAN connectivity. Each of the switch ports used by the L3 device is configured in a different VLAN on the switch. After IP addresses are assigned to the interfaces on the L3 device, the routing table has directly connected routes for all VLANS, and inter-VLAN routing is enabled. The limitations to this approach are the lack of sufficient Fast Ethernet ports on routers, under-utilization of ports on L3 switches and routers, and excessive wiring and manual configuration. The topology used in this lab does not use this approach.

An alternative approach is to create one or more Fast Ethernet connections between the L3 device (the router) and the distribution layer switch, and to configure these connections as dot1q trunks. This allows all inter-VLAN traffic to be carried to and from the routing device on a single trunk. However, it requires that the L3 interface be configured with multiple IP addresses. This can be done by creating "virtual" interfaces, called subinterfaces, on one of the router Fast Ethernet ports and configuring them to dot1q aware.

Using the subinterface configuration approach requires these steps:

1. Enter subinterface configuration mode (e.g., interface fastethernet 0/1.1)
2. Establish trunking encapsulation and associate a VLAN with the subinterface (e.g., for VLAN 1: encapsulation dot1q 1)
3. Assign an IP address from the VLAN to the subinterface

Note the following points in this configuration:

* The subinterface can use any number that can be described with 32 bits, but it is good practice to assign the number of the VLAN as the interface number, as has been done here.
* The native VLAN is specified on the Layer 3 device so that it is consistent with the switches. Otherwise, VLAN 1 would be the native VLAN by default, and there would be no communication between the router and the management VLAN on the switches.

Confirm creation and status of the subinterfaces with the show ip interface brief command:

Are all subinterfaces of FastEthernet0/1 in your output up ?

**Step 4: Configure the server LAN interface on R1.**

R1(config)# interface FastEthernet0/0   
R1(config-if)#ip address 172.x.5.1 255.255.255.0   
R1(config-if)#description server interface

There are now six networks configured. Verify that you can route packets to all six by checking the routing table on R1 using show ip route command.

**Step 5: Verify Inter-VLAN routing.**

From PC1, verify that you can ping the remote server and the other hosts. It may take a couple of pings before the end-to-end path is established.

Are the pings successful and why?

If not, troubleshoot your configuration. Check to make sure that the default gateways have been set on all PCs and all switches. If any of the hosts have gone into hibernation, the connected interface may go down.

**Task 6: Document the devices configurations**

On each device, capture the running configuration to a text file and attach to your report.

**Task 7: Challenge task**

Configure the routing between VLANs when the network has 2 routers connecting to each other. However, in this scenarios, R2 connects to the outside server. You should configure so that the PCs in VLANs attached to R1 can reach the remote server.

**END.**