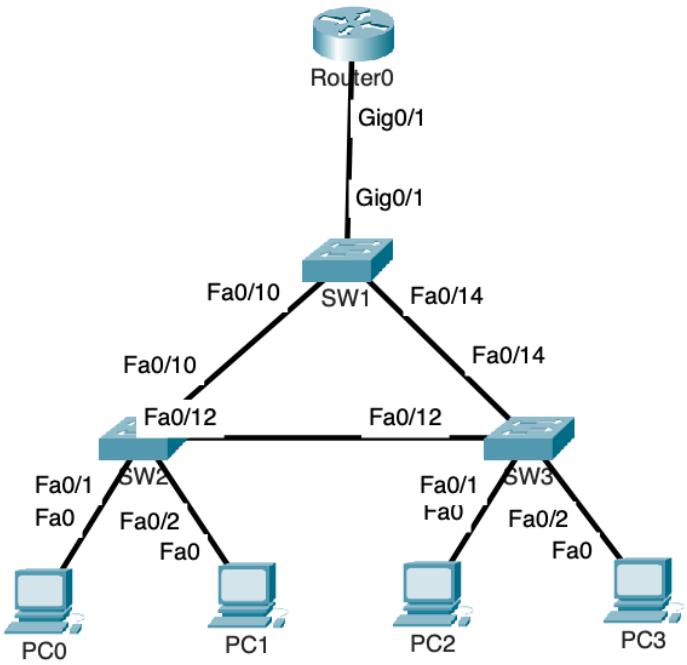
CST337 – Network Configurations and Protocols
Lab 3
Duration: 2 hours

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Lo0	202.10.10.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	
	G0/1.20	192.168.20.1	255.255.255.0	
	G0/1.88	N/A	N/A	
	G0/1.99	192.168.99.1	255.255.255.0	
SW1	VLAN 99	192.168.99.10	255.255.255.0	192.168.99.1
SW2	VLAN 99	192.168.99.11	255.255.255.0	192.168.99.1
SW3	VLAN 99	192.168.99.12	255.255.255.0	192.168.99.1
PC0	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC1	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.12	255.255.255.0	192.168.10.1
PC3	NIC	192.168.20.12	255.255.255.0	192.168.20.1

VLAN and Port Assignments Table

VLAN	Name	Interface
10	Faculty	SW2: F0/1 SW3: F0/1
20	Students	SW2: F0/2 SW3: F0/2
88	Native	SW1: F0/10, F0/14, G0/1 SW2: F0/10, F0/12 SW3: F0/12, F0/14
99	Management	VLAN 99

Required Resources

- 1 Router (Cisco 1941)
- 3 Switches (Cisco 2960)
- 4 PCs
- Console cables to configure the Cisco IOS devices via the console ports.
- Ethernet cables as shown in the topology.

Step 1: Set Up the Topology and Initialize Devices

a. Attach the devices as shown in the topology diagram, and cable as necessary.
b. Power on all the devices in the topology.
c. Initialize and reload the devices.

Step 2: Configure basic device settings for SW1.

a. Console into the SW1 and enable privileged EXEC mode.
b. Enter configuration mode.
c. Assign a device name to the switch.
d. Set SW1's domain name as ccna-lab.com.
e. Disable DNS lookup to prevent SW1 from attempting to translate incorrectly entered commands as though they were host names.
f. Encrypt the plaintext passwords.
g. Configure the username **SSHadmin** with an encrypted password of **SSHadmin!2023**.
h. Generate a set of crypto keys with a 1024 bit modulus
i. Assign the privileged EXEC password to **CiscoPRIV!2023**
j. Assign **CiscoCON!2023** as the console password, configure sessions to disconnect after four minutes of inactivity, and enable login.
k. Assign **CiscoVTY!2023** as the vty password, configure the vty lines to accept SSH connections only, configure sessions to disconnect after four minutes of inactivity, and enable login using the local database.
l. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

Step 3: Configure Host Addressing

a. Configure the NIC interfaces of hosts in the network with the IP addresses given in the Addressing Table.

Step 4: Create and name VLANs on SW1, SW2 and SW3.

a. Create and name the VLANs based on the VLAN and port assignments table.

Step 5: Assign VLANs to the active ports on SW2 and SW3.

a. Configure the interfaces as access ports and assign the VLANs based on based on the VLAN and port assignments table.

Step 6: Configure trunking on SW1, SW2 and SW3 and use VLAN 88 as the native VLAN.

a. Configure interfaces on SW1, SW2, and SW3 for trunking based on the VLAN and port assignments table.

Step 7: Configure management VLAN on SW1, SW2 and SW3.

a. Configure management VLAN on SW1, SW2, and SW3.
b. Assign the IP address for the management VLAN based on Addressing Table.
c. Configure the default gateway on SW1, SW2 and SW3.

Step 8: Configure rapid-PVST on SW1, SW2 and SW3.

a. Configure per-VLAN rapid spanning tree mode on SW1, SW2, and SW3.

Step 9: Configure inter-VLAN routing on the router.

a. Activate interface G0/1 on the router.

```
R1(config)# interface g0/1
R1(config-if)# no shutdown
R1(config-if)# exit
```

b. Configure sub-interfaces for each VLAN as specified in the IP addressing table. All sub-interfaces use 802.1Q encapsulation. Ensure the sub-interface for the native VLAN does not have an IP address assigned. Include a description for each sub-interface.

```
R1(config)# interface g0/1.10
R1(config-subif)# description faculty network
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)# description students network
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# interface g0/1.88
R1(config-subif)# encapsulation dot1q 88 native
R1(config-subif)# description Native VLAN
R1(config-subif)# interface g0/1.99
R1(config-subif)# encapsulation dot1q 99
R1(config-subif)# description management
R1(config-subif)# ip address 192.168.99.1 255.255.255.0
```

Step 10: Verify network connectivity.

LAB INSTRUCTIONS:

1. You are required to complete the configuration based on the instruction.
2. Marks will be given only after you complete the configuration and the link between PCs can be established.