**LAB 8 - IMPLEMENT VLANS AND TRUNKING**

**Course Code - Course Name:** - COMP4039 – Network Foundations

**Program:** T433 - Cybersecurity

**Section:** A

**Term:** - Winter 2024

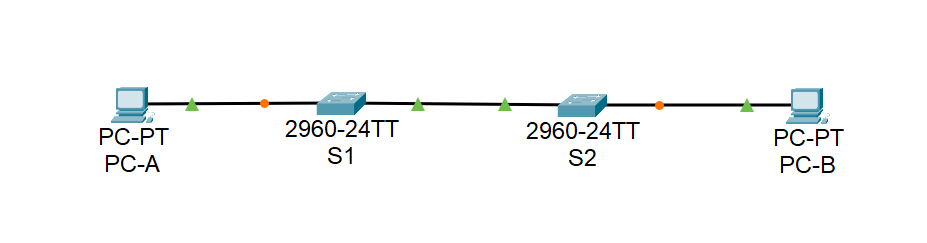
**Group Number:** 06

**Student Names - ID:**

* Prabhjot Singh Sains – 101495218
* Rahul Patel - 101378458
* Jai Deep Rawat - 101503760
* M. Salmaan Mustafa Shah – 10151007

**Lab Report by -** Prabhjot Singh Sains

**Topology**



**Addressing table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| S1 | VLAN 10 | 192.168.10.11 | 255.255.255.0 |
| VLAN 20 | 192.168.20.11 | 255.255.255.0 |
| VLAN 30 | 192.168.30.11 | 255.255.255.0 |
| S2 | VLAN 10 | 192.168.10.12 | 255.255.255.0 |
| PC-A | NIC | 192.168.20.13 | 255.255.255.0 |
| PC-B | NIC | 192.168.30.13 | 255.255.255.0 |

**VLAN Table**

|  |  |  |
| --- | --- | --- |
| **VLAN** | **NAME** | **Interface assigned** |
| 10 | Management | S1: VLAN 10  S2: VLAN 10 |
| 20 | Sales | S1: VLAN 20 and F0/6 |
| 30 | Operation | S1: VLAN 30  S2: F0/18 |
| 999 | ParkingLot | S1: F0/2-5, F0/7-24, G0/1-2  S2: F0/2-17, F0/19-24, G0/1-2 |
| 1000 | Native | N/A |

**Instructions**

**Part A: Set up the topology and initialize the devices:**

1. Cable the network as shown in the topology diagram and turn on your devices.
2. Connect the rollover console cable to the RJ-45 console port of the switches S1 and S2 and start any available emulation program such as (Tera Term, putty, or Hyper Terminal)
3. Initialize and reload the switches to clear any existing configuration using the following commands:

Switch> enable

Switch# delete vlan.dat

Switch# erase startup-config

Switch# reload

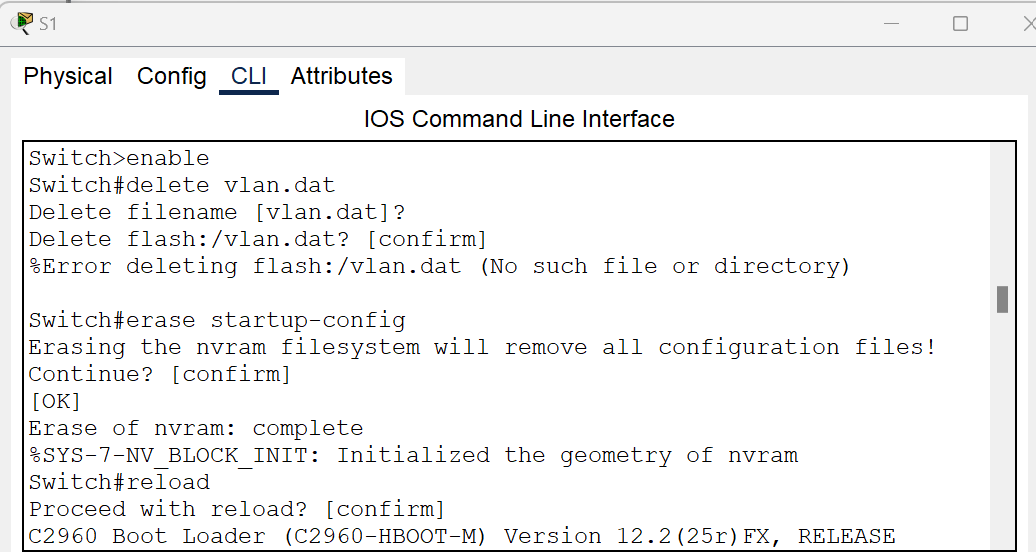


Fig 1 - S1

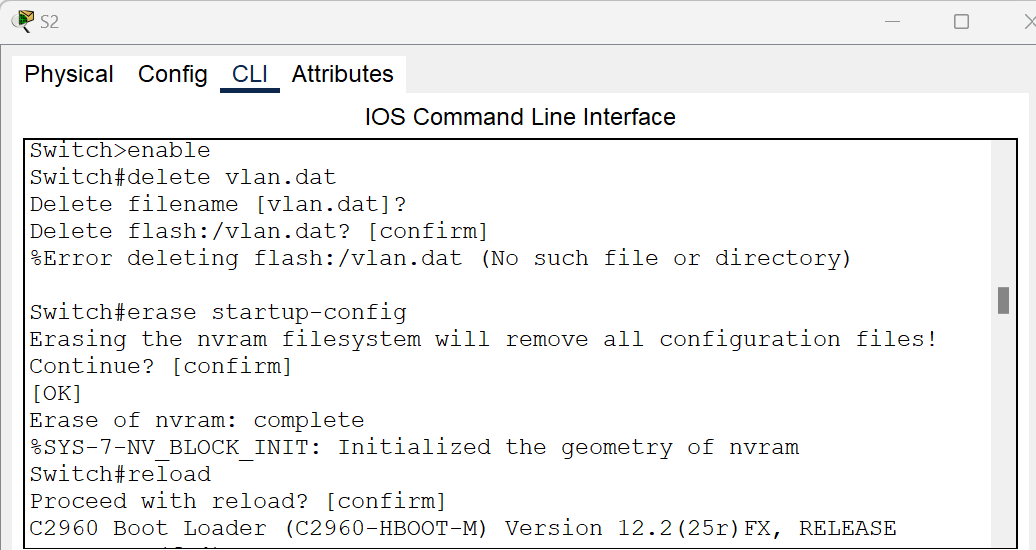


Fig 2 – S2

**Part B: Configure basic configuration and verify connectivity:**

1. Console into the switch and enable privileged EXEC mode: use the enable command then use the configure terminal command to navigate to global configuration mode.

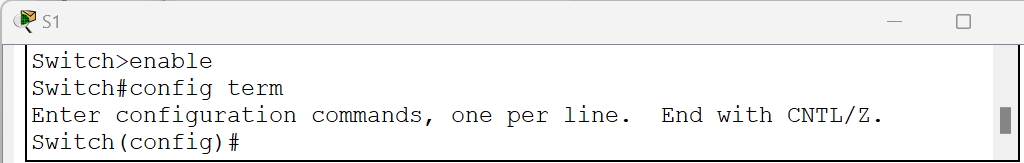


Fig 3 - S1

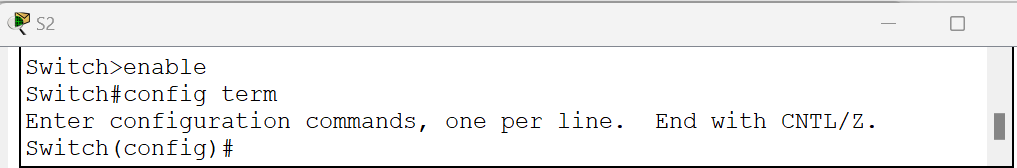


Fig 4 – S2

1. Use the hostname command to change the switches' names to S1 and S2. The commands provided as a sample for S1, you should do the same for S2.

switch (config)# hostname S1

S1(config)#

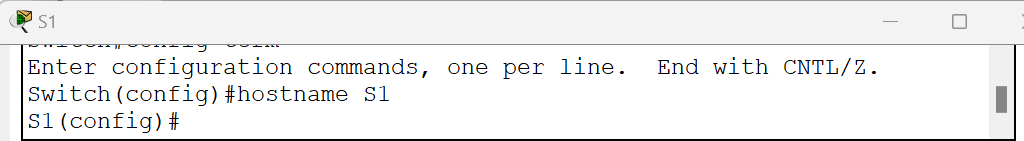


Fig 5 - S1

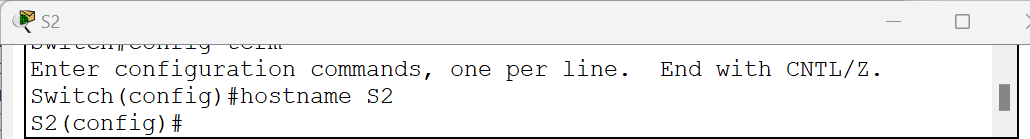


Fig 6 – S2

1. Disable DNS lookup to prevent unwanted DNS lookups.

S1(config)# no ip domain-lookup

S2(config)# no ip domain-lookup

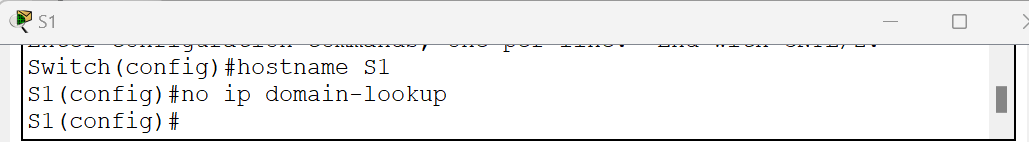


Fig 7 - S1

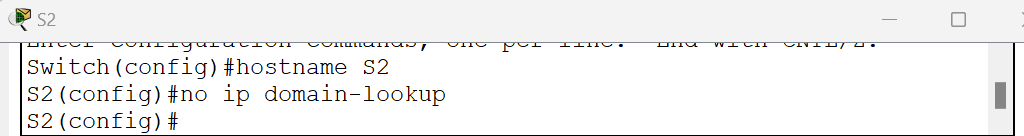


Fig 8 – S2

1. Assign the class as the privileged EXEC encrypted password.

S1(config)# enable secret class

S2(config)# enable secret class

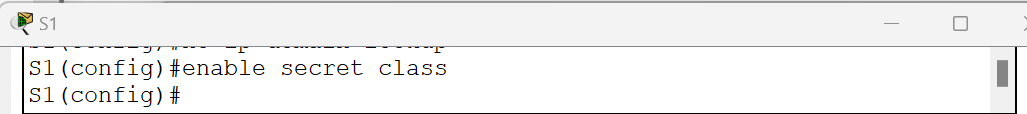


Fig 9 - S1



Fig 10 – S2

1. Assign Cisco as the console password and enable login.

S1(config)# line con 0

S1(config-line)# password cisco

S1(config-line)# login

S1(config-line)# exit

S1(config)#

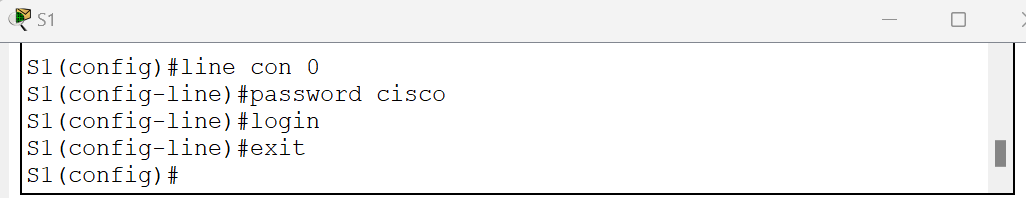


Fig 11 – S1

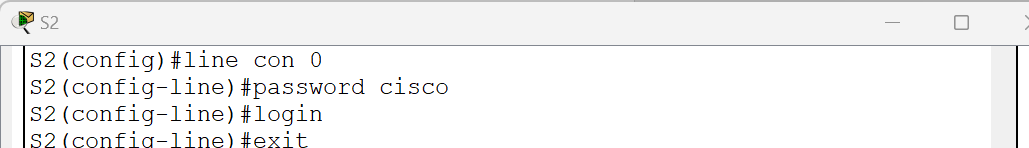


Fig 12 – S2

1. Assign Cisco as the VTY password and enable login.

S1(config)# line vty 0 15

S1(config-line)# password cisco

S1(config-line)# login

S1(config-line)# exit

S1(config)#

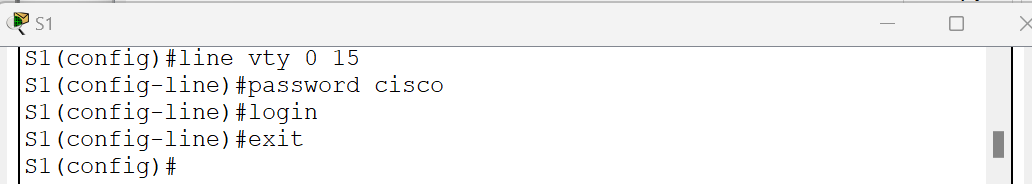


Fig 13 – S1

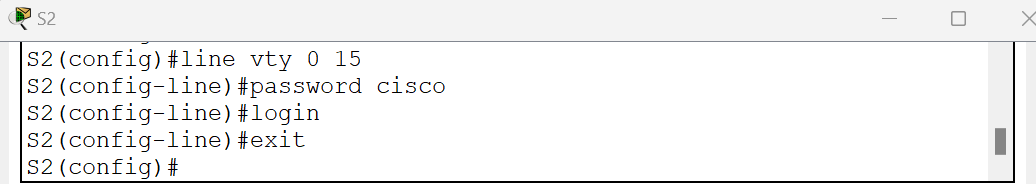


Fig 14– S2

1. Encrypt the plaintext passwords.

S1(config)# service password-encryption



Fig 15 – S1

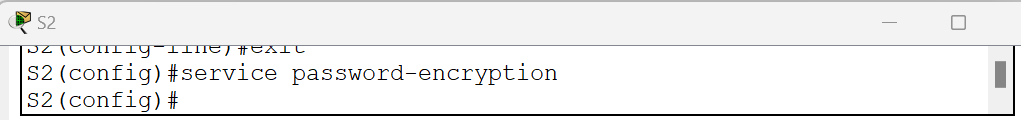


Fig 16 – S2

1. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# banner motd # Unauthorized access is strictly prohibited. #

S1(config)# exit

S1#

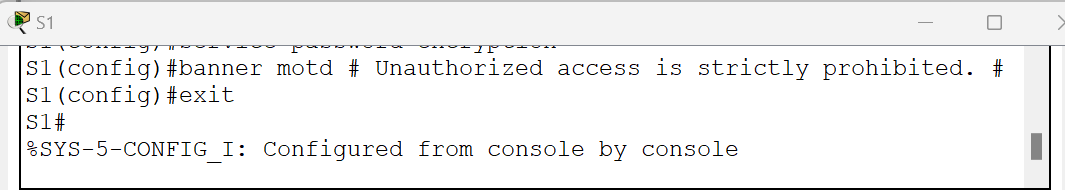


Fig 17 – S1

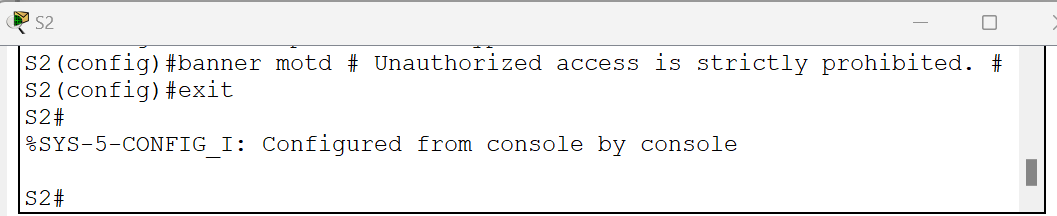


Fig 18 – S2

1. Save the configuration. Use the copy command to save the running configuration to the startup file on non-volatile random-access memory (NVRAM).

R# copy running-config startup-config

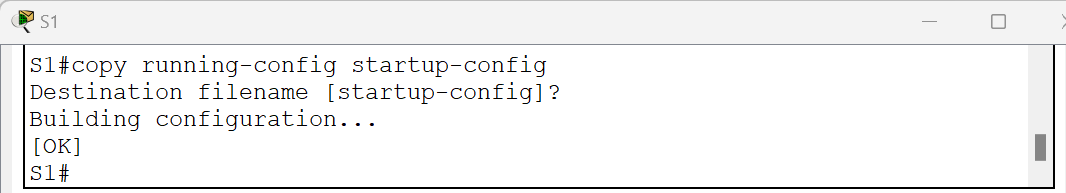


Fig 19 – S1

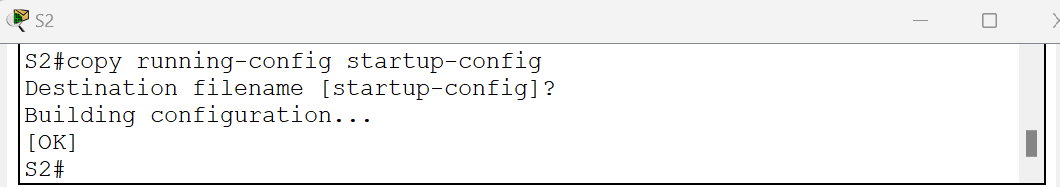


Fig 20 – S2

1. Configure PC hosts: Refer to the Addressing Table for PC host address information

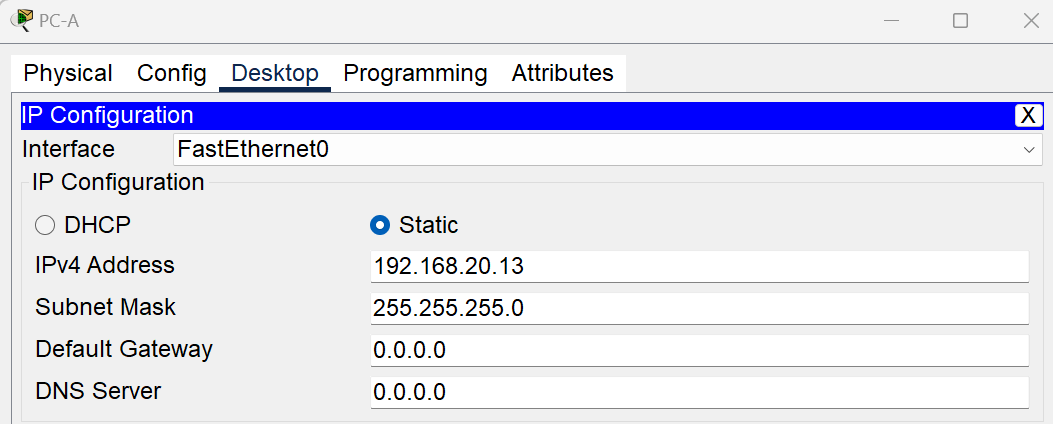


Fig 21 – PC-A

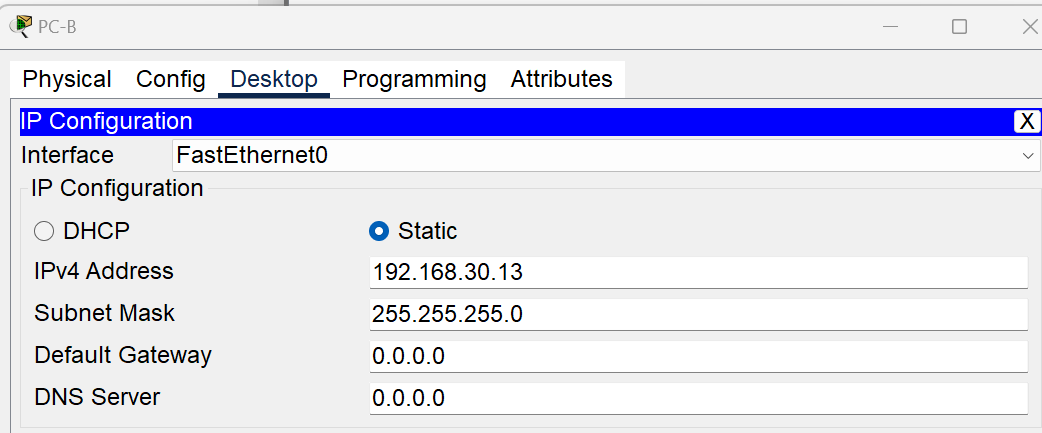


Fig 22 – PC-B

1. Configure an IP address on both switches for SVI (VLAN 1), refer to the addressing table.

S1(config)# interface vlan 1

S1(config-if)# ip address 192.168.1.1 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# exit

S1(config)# exit

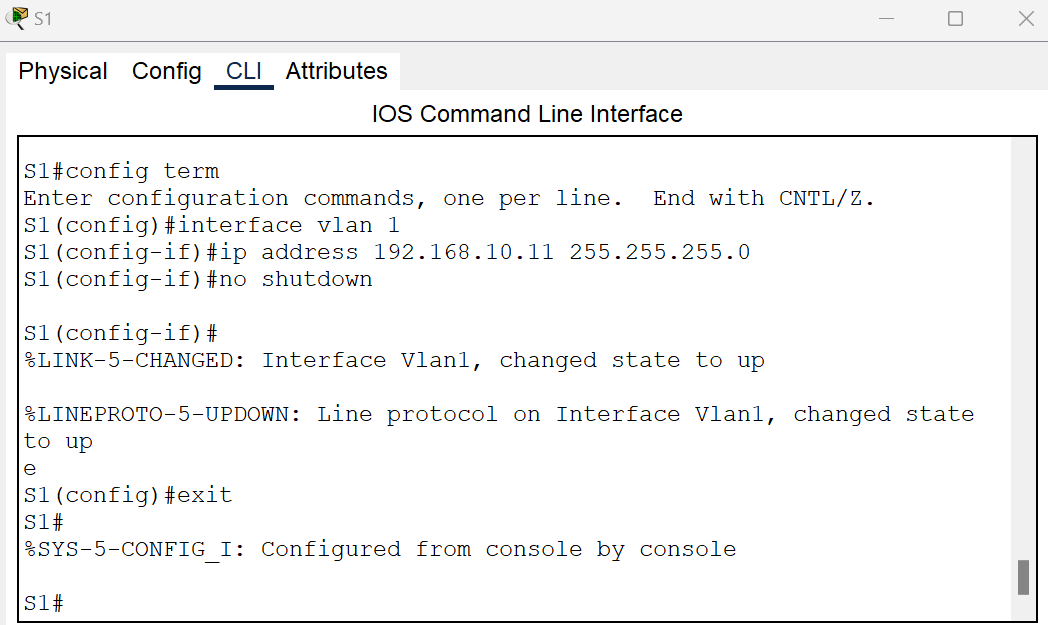


Fig 23 – S1

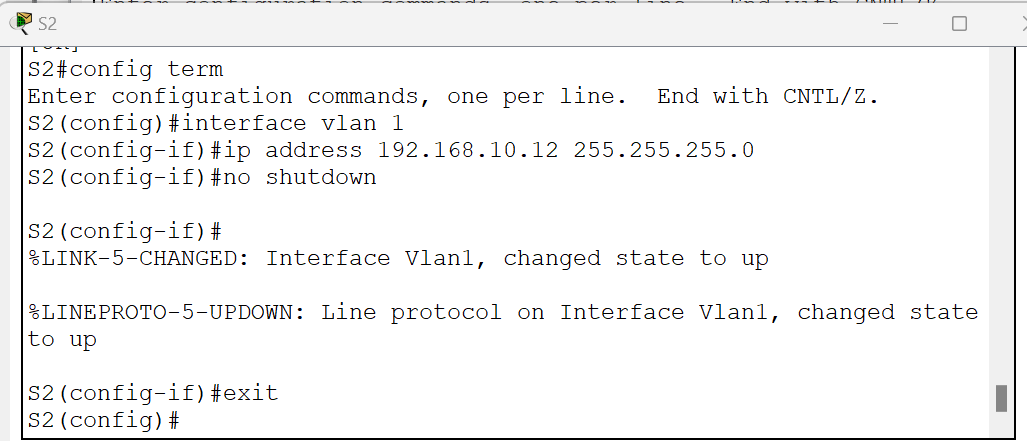


Fig 24 – S2

1. Test the connectivity between PCA and PCB, and troubleshoot as necessary.

Use the command prompt (cmd.exe) window to verify the connectivity between PCs.

From PC-A Type >ping 192.168.2.3 and press Enter. Were the ping results successful? No

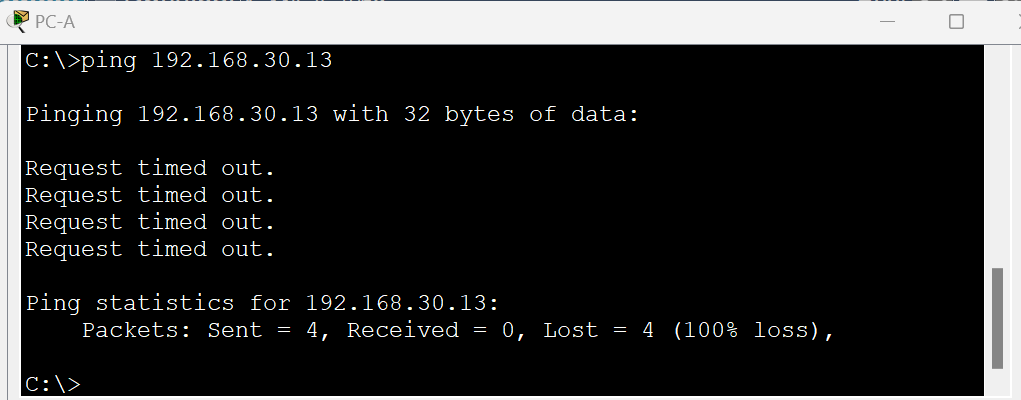


Fig 25 – PC-A

From PC-B Type >ping 192.168.1.3 and press Enter. Were the ping results successful? No

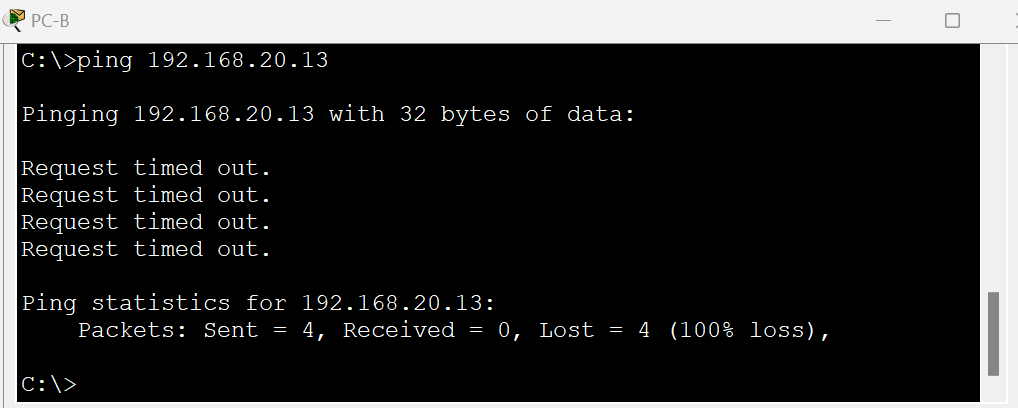


Fig 26 – PC-B

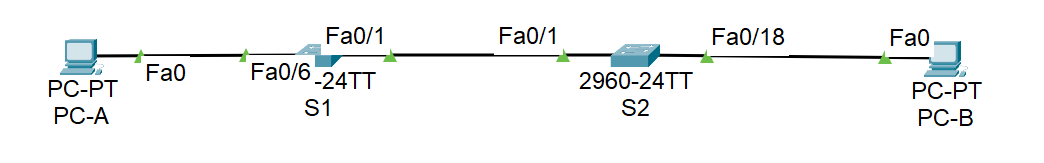


Fig 27 – Topology

**Part C: Create VLANs and Assign Switch Ports:**

1. Create and name the required VLANs on each switch from the table above. Use the VLAN command.

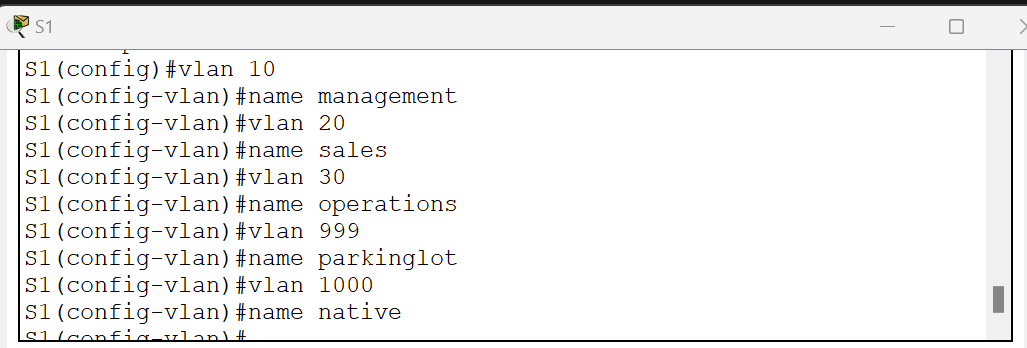


Fig 28 – S1

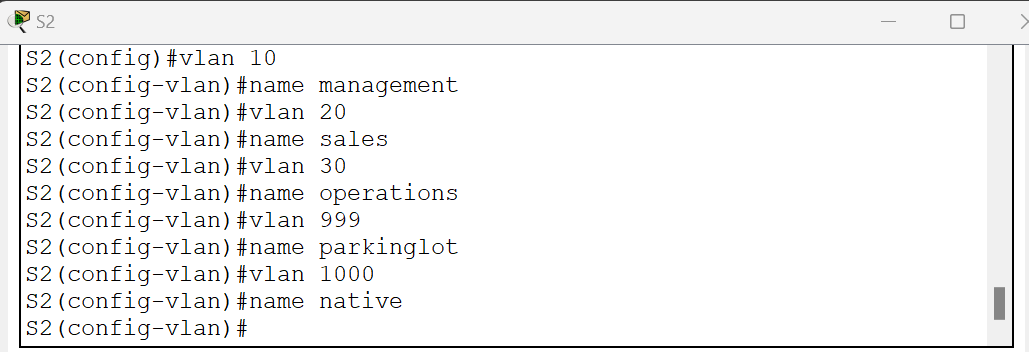


Fig 29– S2

1. Configure the management interface on each switch using the IP address information in the Addressing Table.

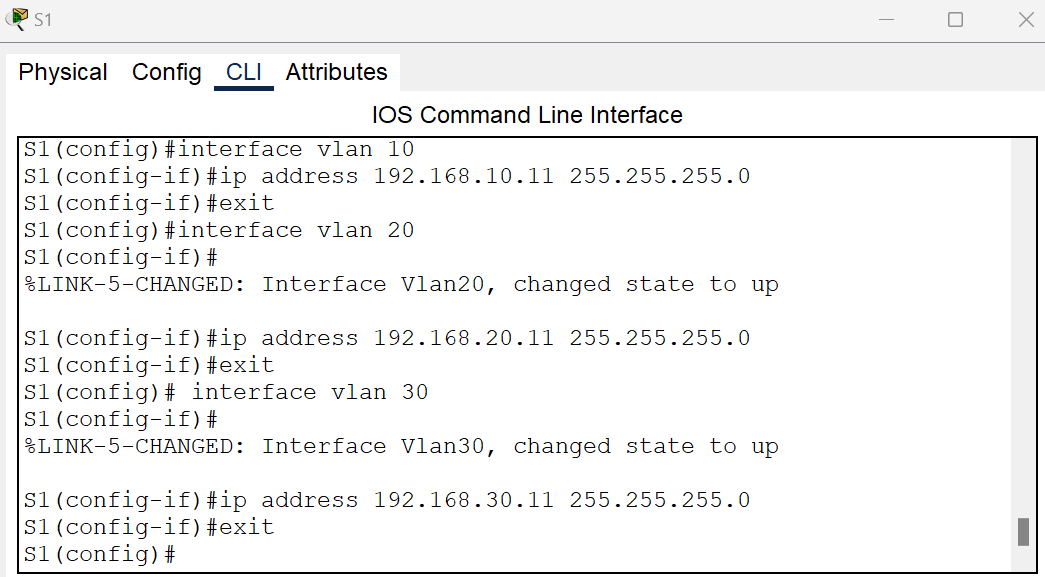


Fig 30 – S1

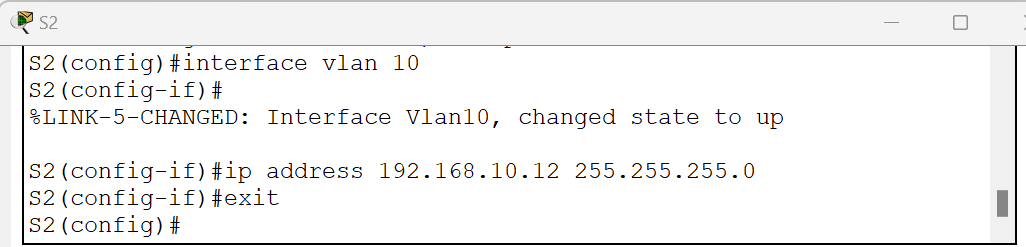


Fig 31 – S2

1. Assign all unused ports on the switch to the ParkingLot VLAN, configure them for static access mode, and administratively deactivate them.

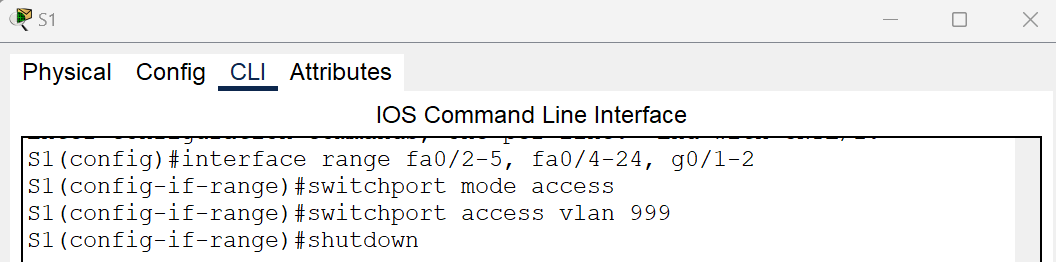


Fig 31 – S1

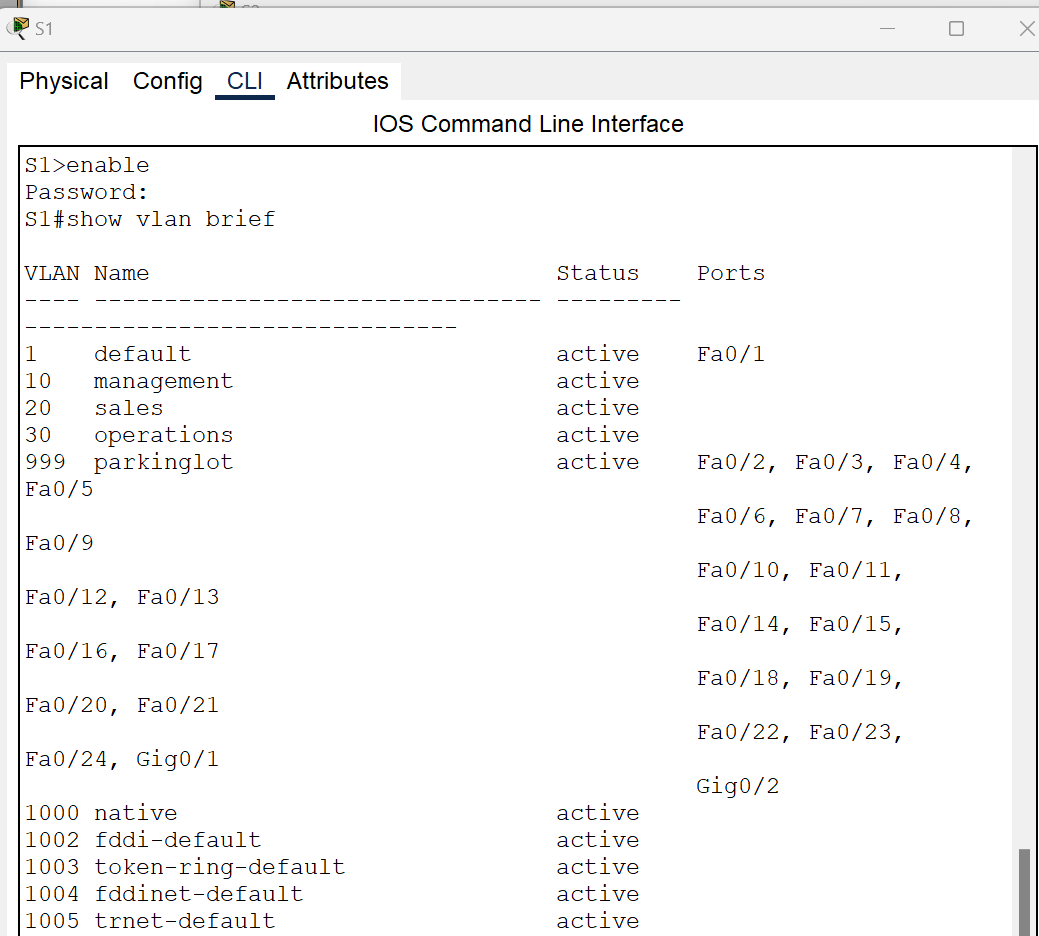


Fig 32 – S1

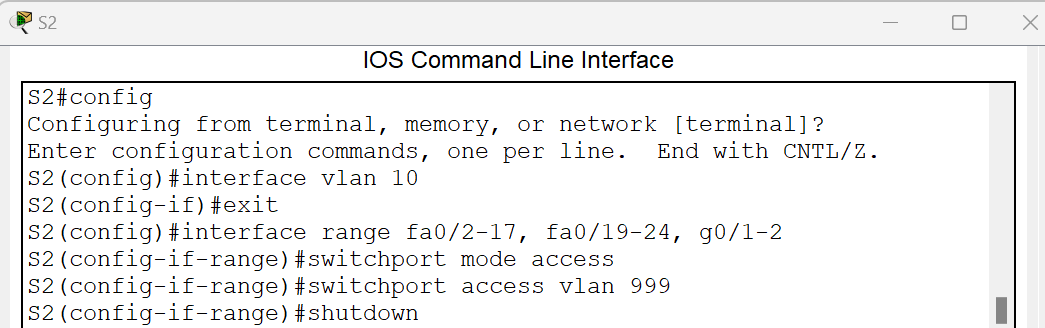


Fig 33 – S2

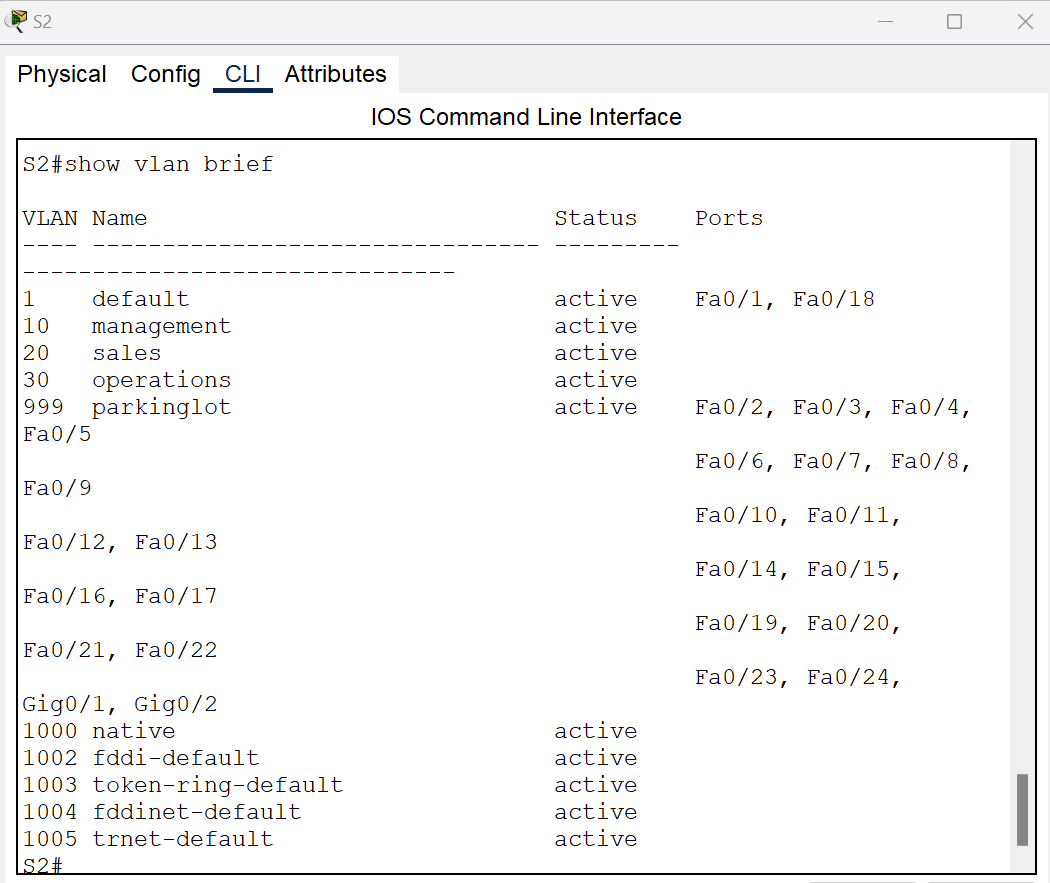


Fig 34 – S2

1. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.

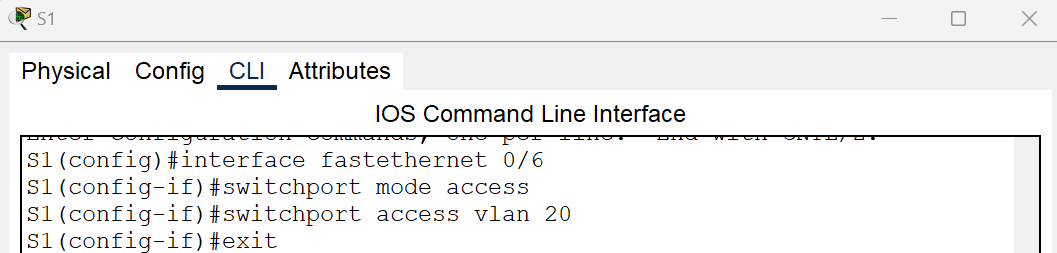


Fig 35 – S1

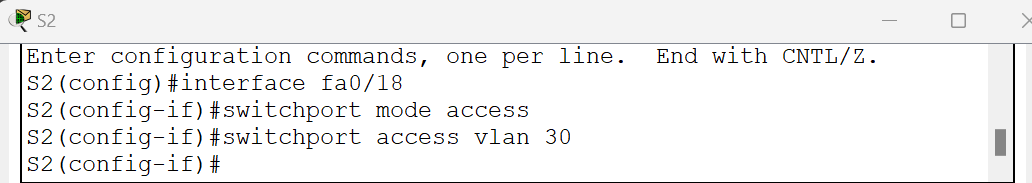


Fig 36 – S2

1. Verify that the VLANs are assigned to the correct interfaces.

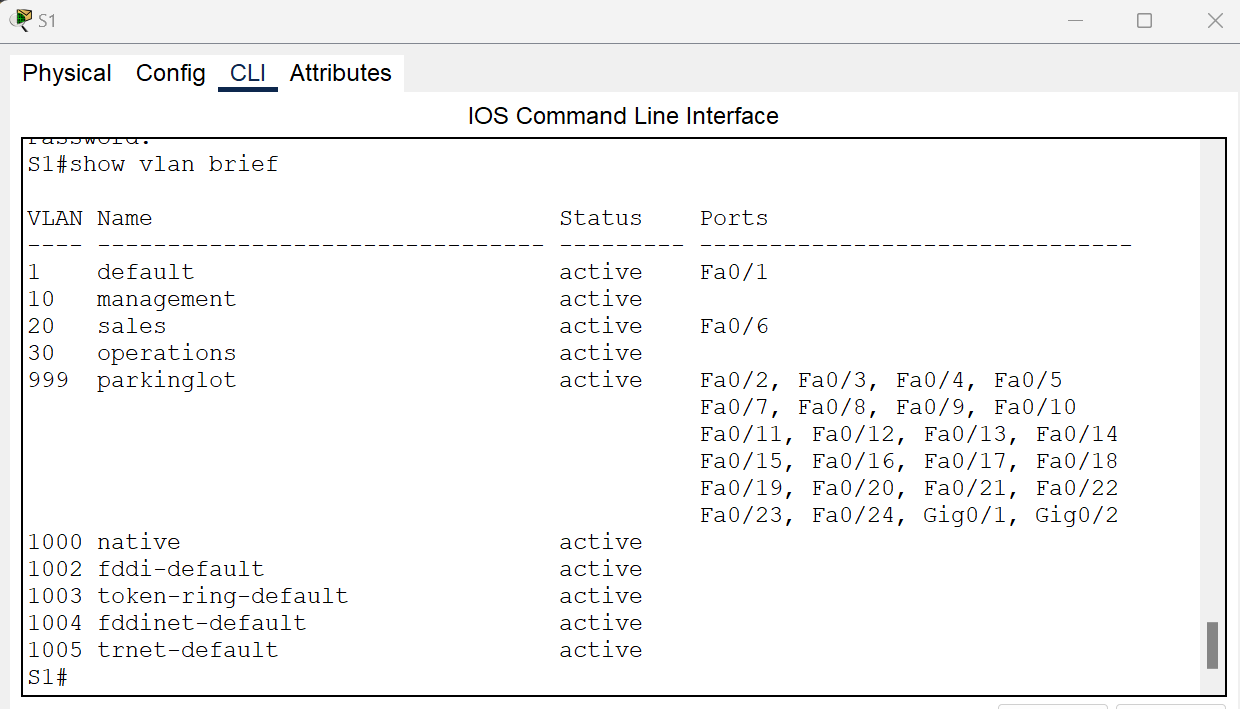


Fig 37 – S1

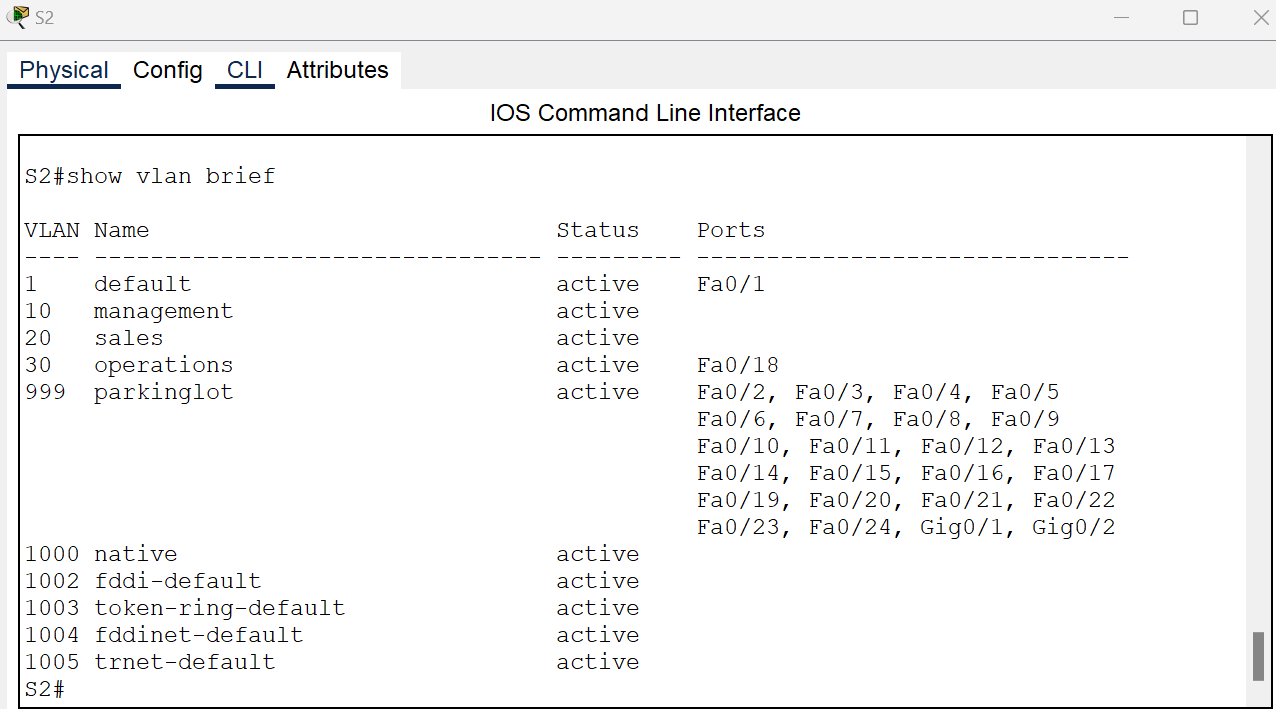


Fig 38 – S2

1. Manually configure trunk interface F0/1 on both switches.

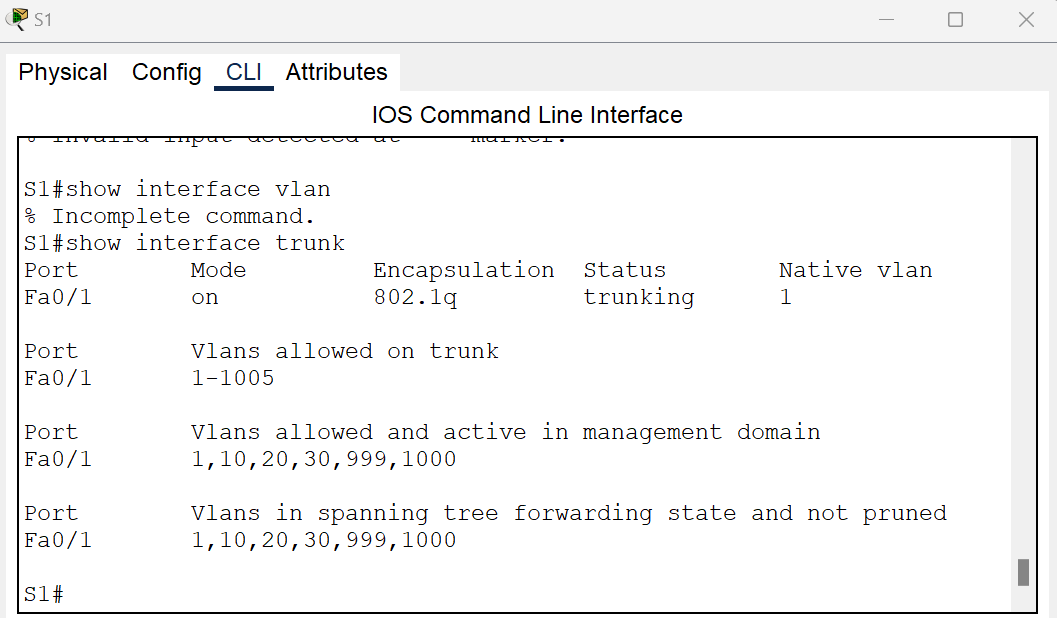


Fig 39 – S1

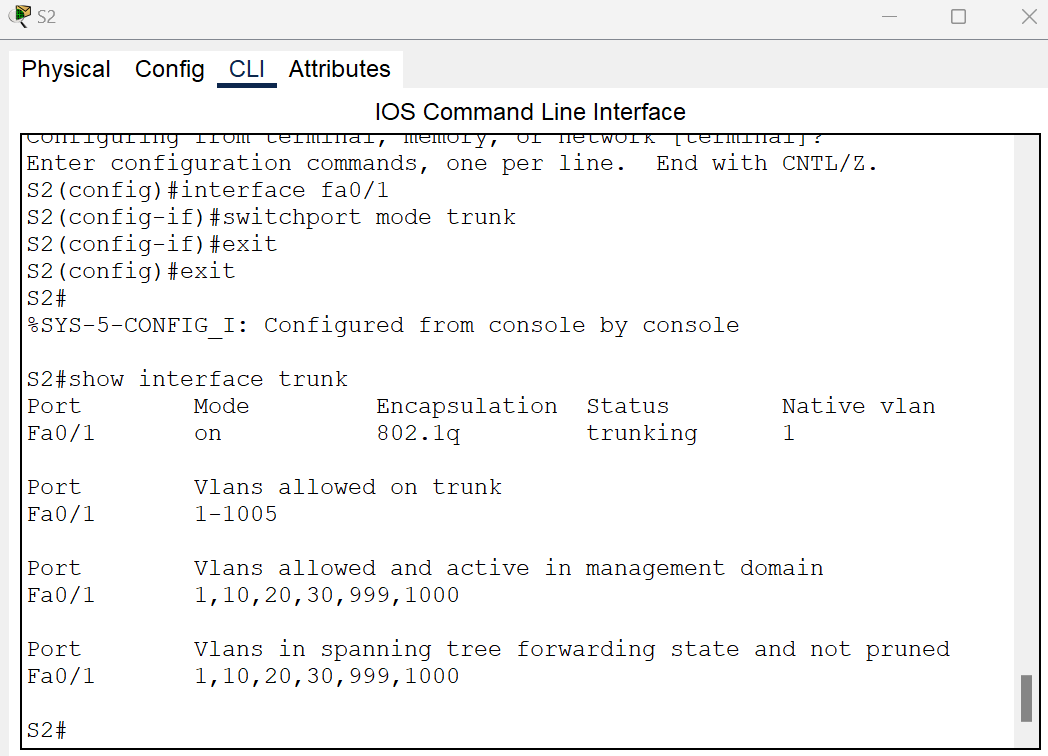


Fig 40 – S2

1. Set the native VLAN to 1000 on both switches.

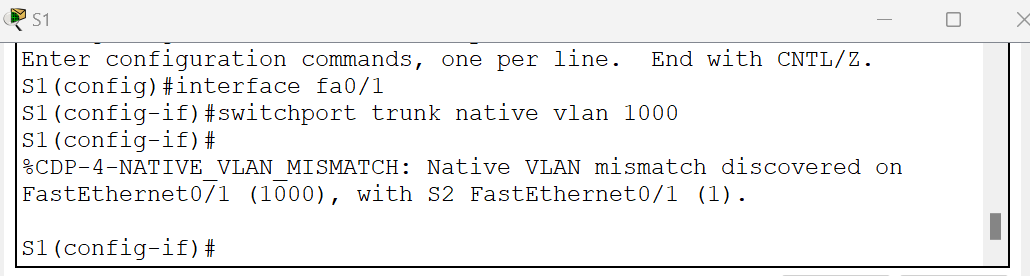


Fig 41 – S1

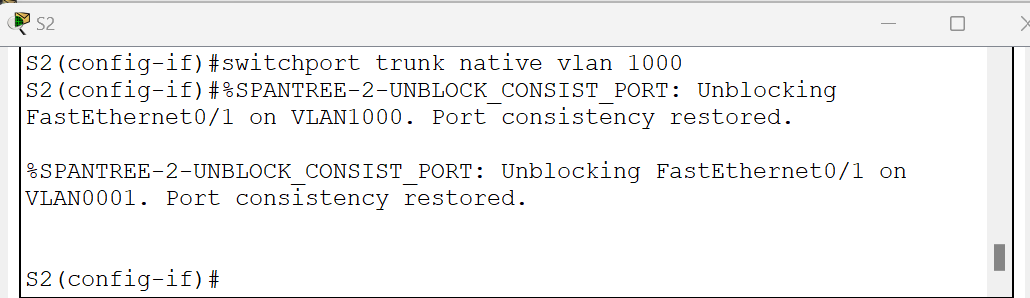


Fig 42 – S2

1. specify that only VLANs 10, 20, 30, and 1000 are allowed to cross the trunk.

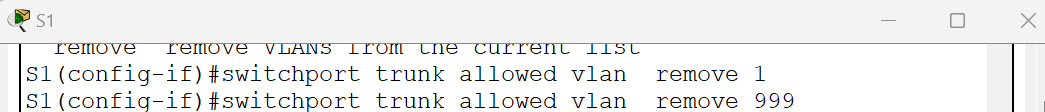


Fig 43 – S1

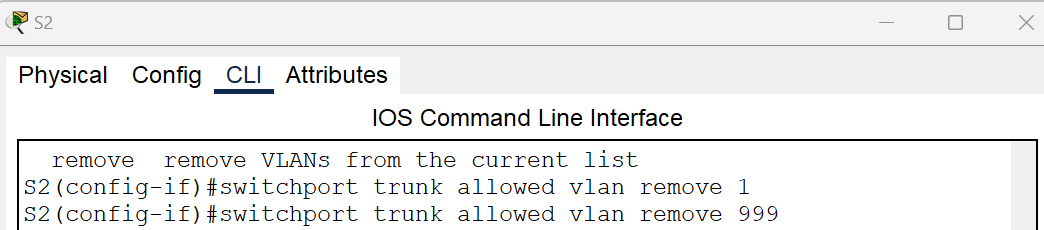


Fig 44 – S2

1. Issue the show interfaces trunk command to verify trunking ports, the native VLAN, and allowed VLANs across the trunk.

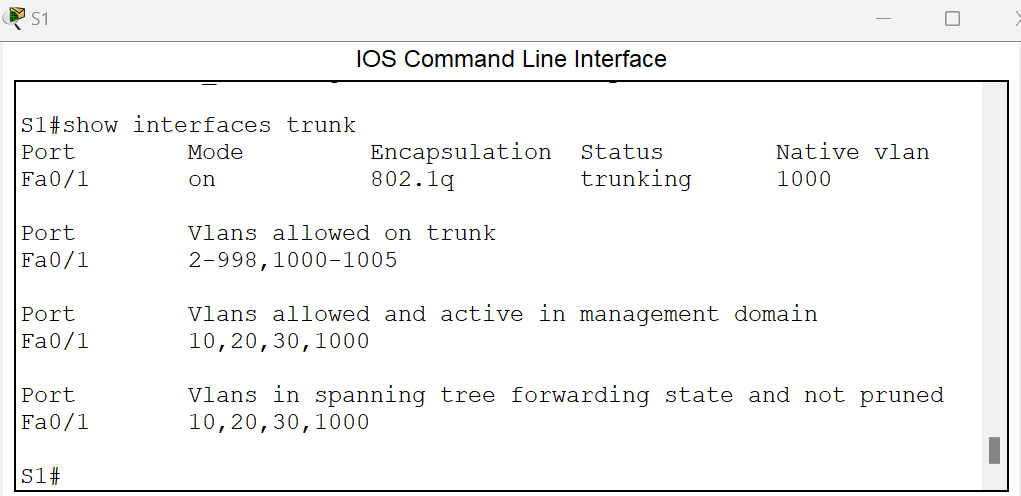


Fig 45 – S1

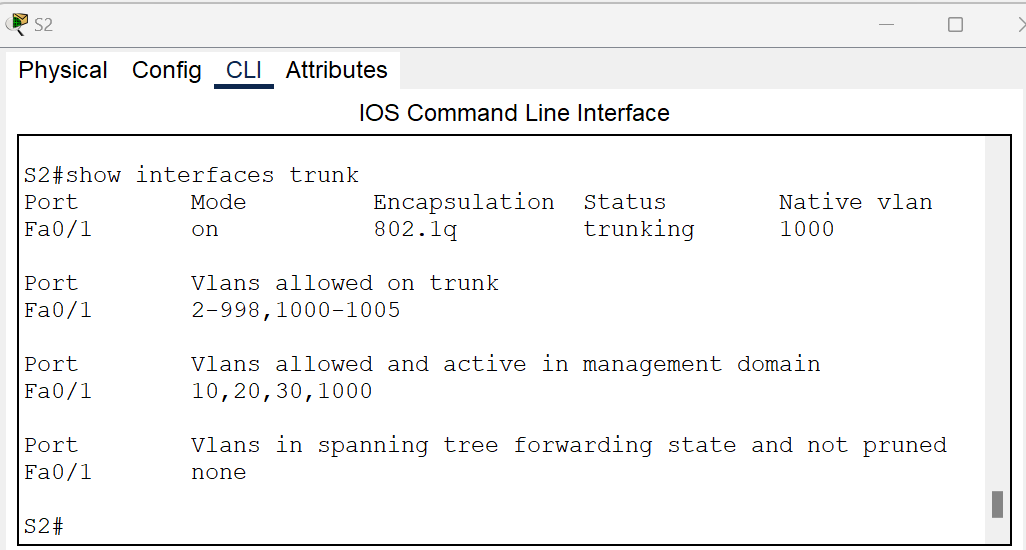


Fig 46 – S2

1. Verify connectivity within a VLAN. For example, PC-A should be able to ping S1 VLAN 20 successfully.

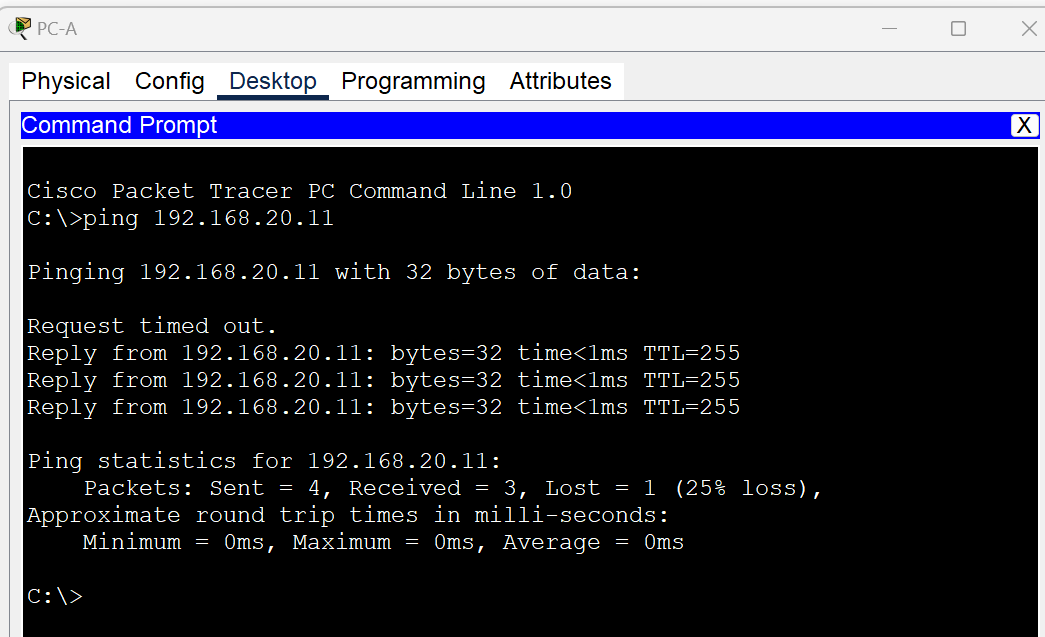


Fig 47 –Ping