Implement Inter-VLAN Routing

**Part 1:   Build the Network and Configure Basic Device Settings**

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

**Step 1:  Cable the network as shown in the topology and Addressing table.**

Attach the devices as shown in the topology diagram, and cable as necessary.

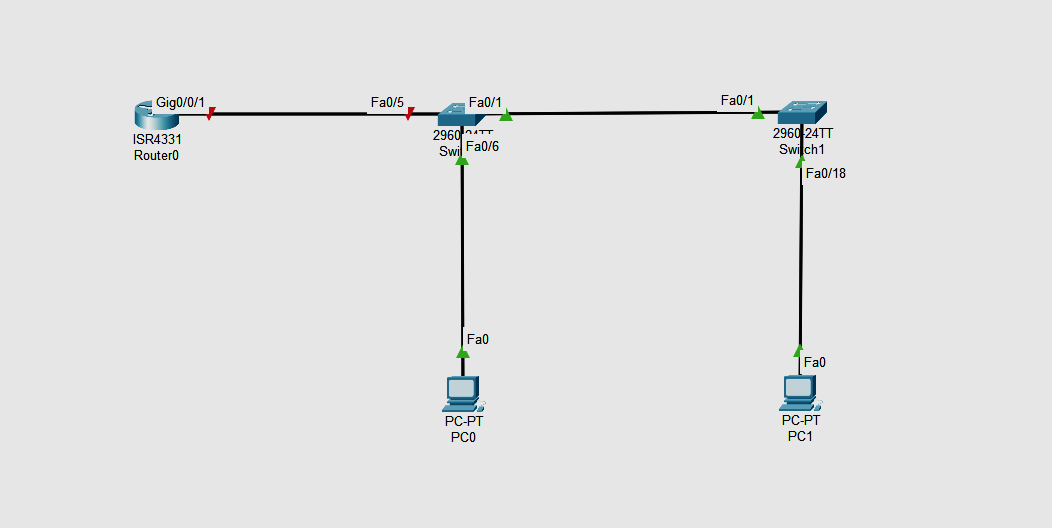
# Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- | --- |
| R1 | G0/0/1.10 | 192.168.10.1 | 255.255.255.0 | N/A |
| *R1* | G0/0/1.20 | 192.168.20.1 | 255.255.255.0 | *N/A* |
| *R1* | G0/0/1.30 | 192.168.30.1 | 255.255.255.0 | *N/A* |
| *R1* | G0/0/1.1000 | N/A | N/A | *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 | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |
| PC-B | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

# VLAN Table

| **VLAN** | **Name** | **Interface Assigned** |
| --- | --- | --- |
| 10 | Management | S1: VLAN 10  S2: VLAN 10 |
| 20 | Sales | S1: F0/6 |
| 30 | Operations | S2: F0/18 |
| 999 | Parking\_Lot | S1: F0/2-4, F0/7-24, G0/1-2  S2: F0/2-17, F0/19-24, G0/1-2 |
| 1000 | Native | N/A |

**Topology**



**Step 2:  Configure basic settings for the router.**

router> enable

router# config terminal

router(config)# hostname R1

**Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.**

R1(config)# no ip domain lookup

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

R1(config)# enable secret class

**Assign cisco as the console password and enable login.**

R1(config)# line console 0

R1(config-line)# password cisco

R1(config-line)# login

**Assign cisco as the vty password and enable login.**

R1(config)# line vty 0 4

R1(config-line)# password cisco

R1(config-line)# login

**Encrypt the plaintext passwords.**

R1(config)# service password-encryption

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

R1(config)# **banner motd $ Authorized Users Only! $**

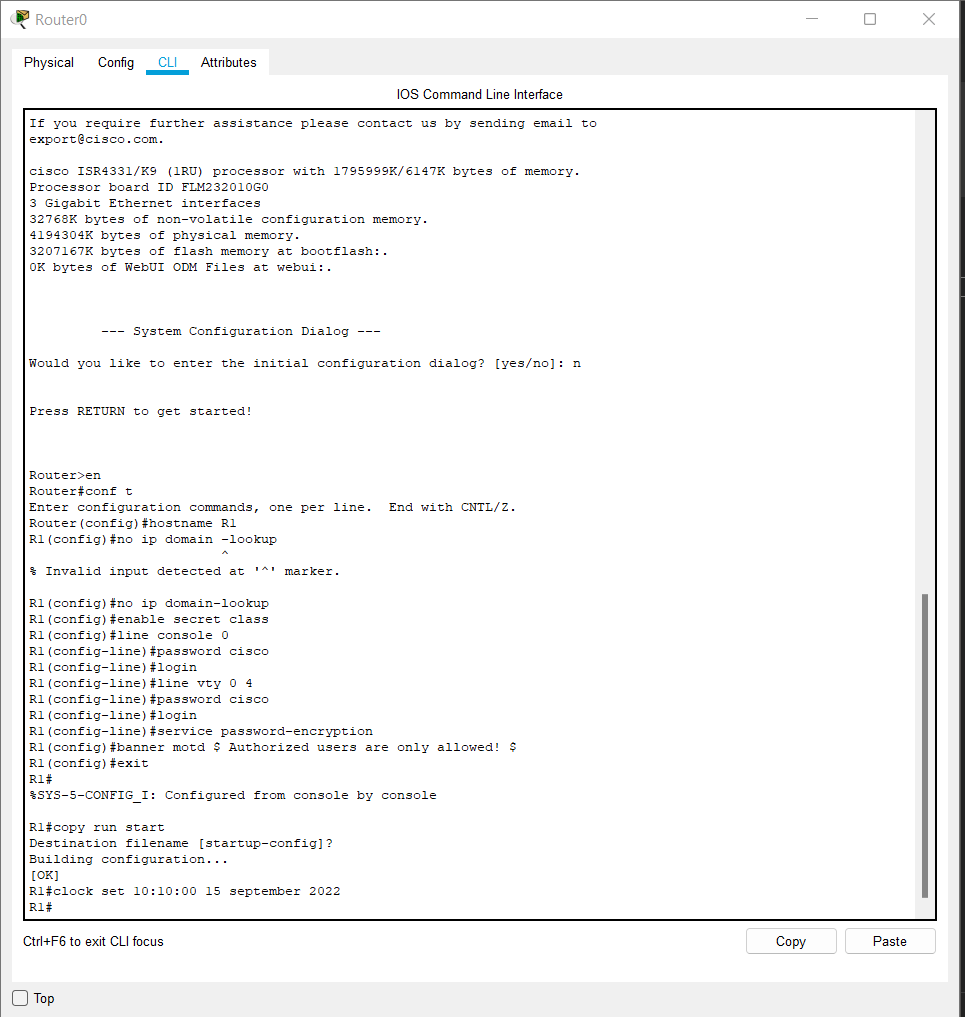
**Save the running configuration to the startup configuration file.**

R1(config)# **exit**

R1# **copy running-config startup-config**

**Set the clock on the router**.

R1# **clock set 10:10:00 15 september 2022**



**Step 3:  Configure basic settings for each switch.**

1. Assign a device name to the switch.

switch(config)# **hostname S1**

switch(config)# **hostname S2**

1. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

S1(config)# **no ip domain-lookup**

S2(config)# **no ip domain-lookup**

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

S1(config)# **enable secret class**

S2(config)# **enable secret class**

1. Assign **cisco** as the console password and enable login.

S1(config)# **line console 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S2(config)# **line console 0**

S2(config-line)# **password cisco**

S2(config-line)# **login**

1. Assign **cisco** as the vty password and enable login.

S1(config)# **line vty 0 4**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S2(config)# **line vty 0 4**

S2(config-line)# **password cisco**

S2(config-line)# **login**

1. Encrypt the plaintext passwords.

S1(config)# **service password-encryption**

S2(config)# **service password-encryption**

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

S1(config)# **banner motd $ Authorized Users Only! $**

S2(config)# **exit**

S2(config)# **banner motd $ Authorized Users Only! $**

S2(config)# **exit**

1. Set the clock on the switch.

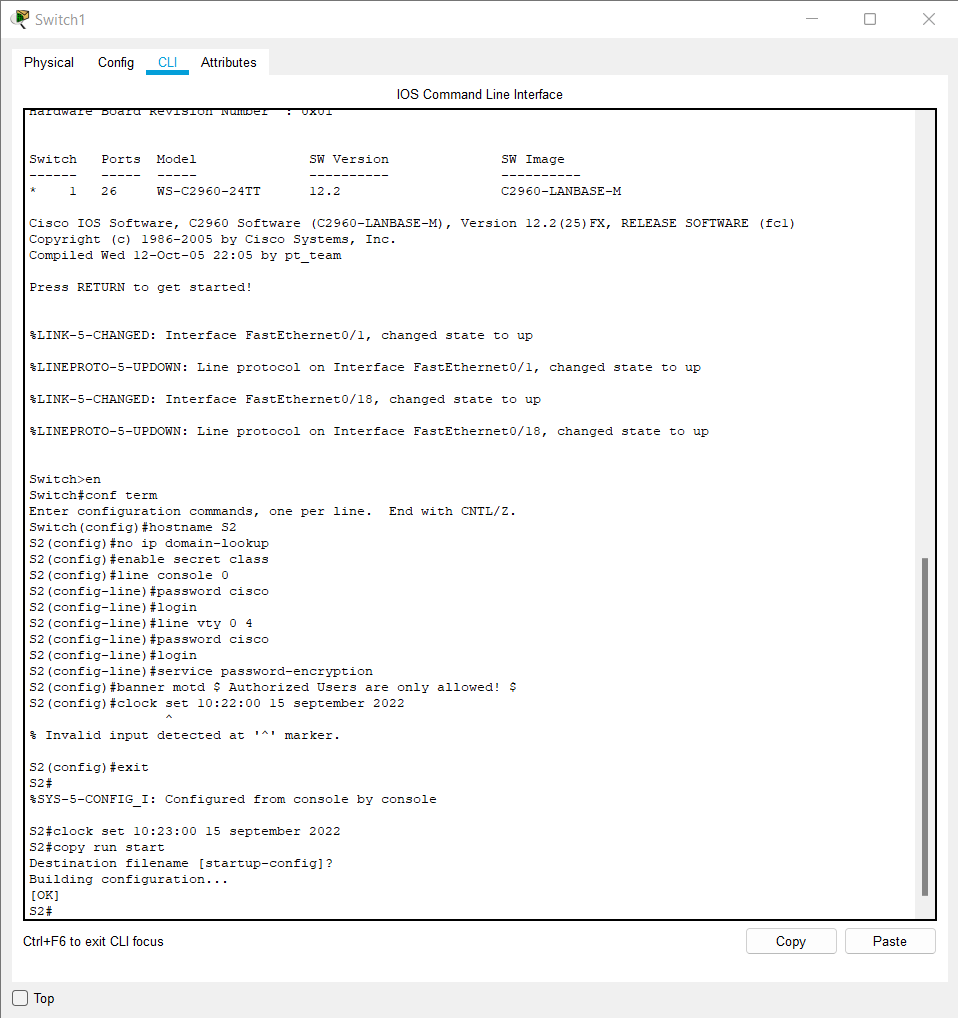
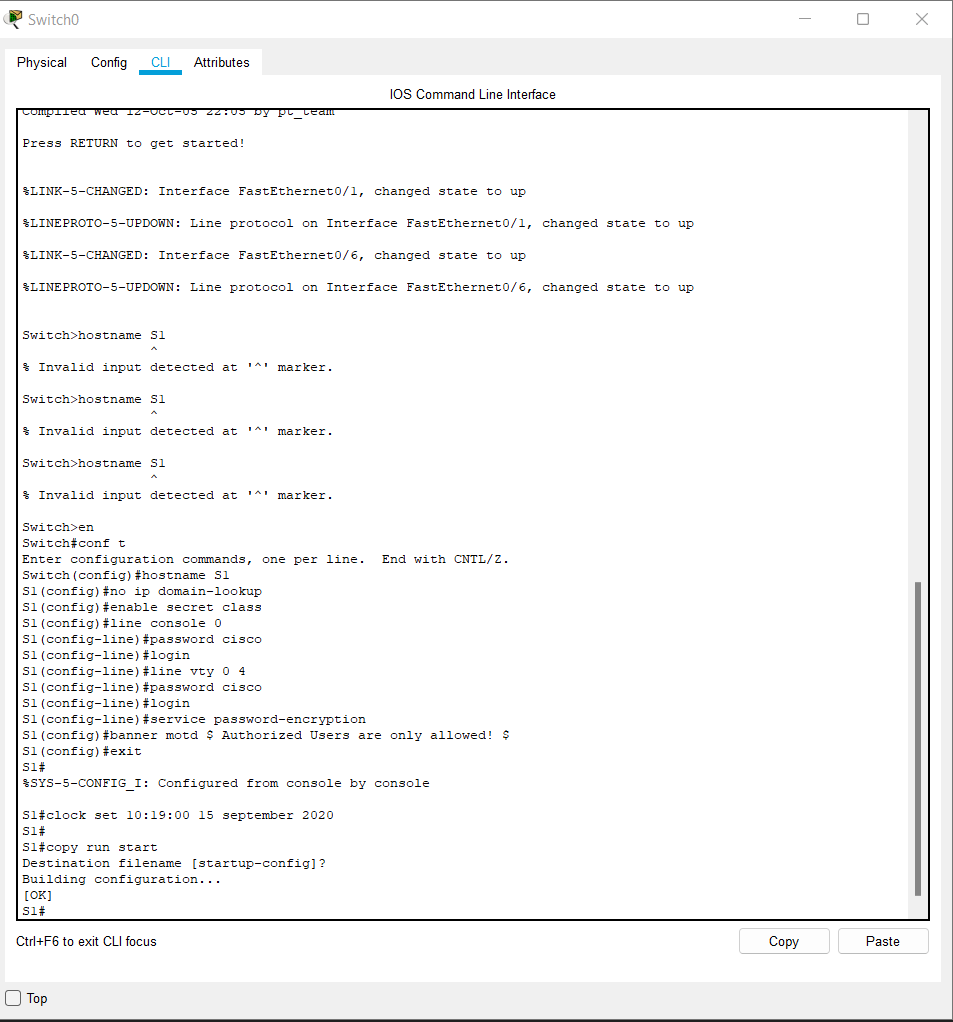
S1# **clock set 15:30:00 27 Aug 2019**

S2# **clock set 15:30:00 27 Aug 2019**

1. Save the running configuration to the startup configuration.

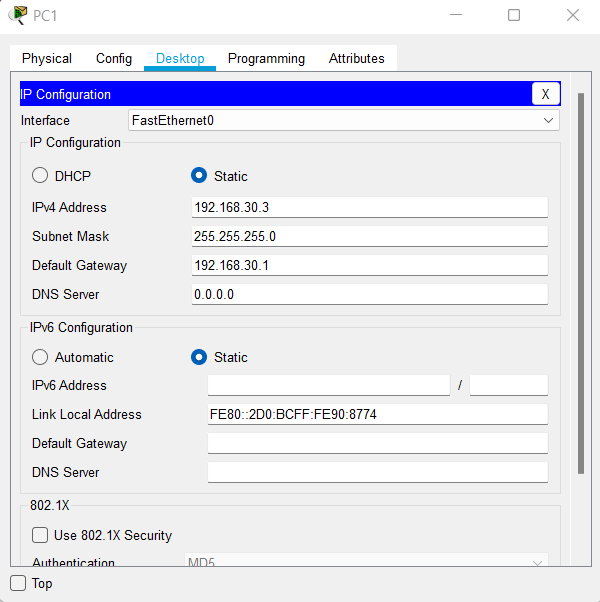
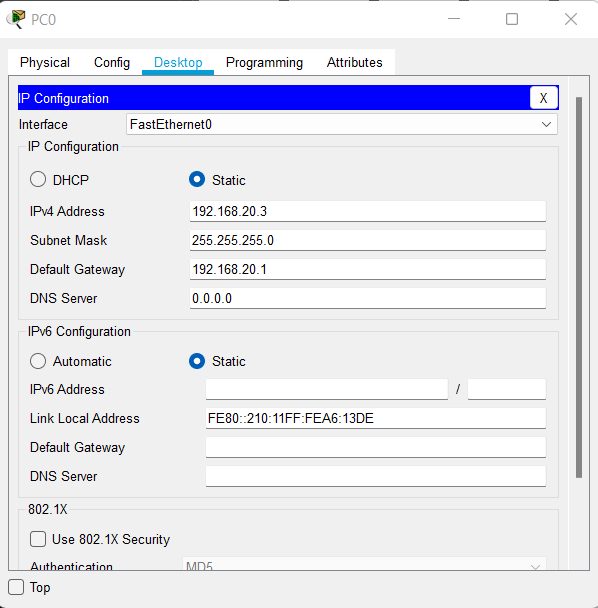
S1# **copy running-config startup-config**

S2# **copy running-config startup-config**



**Step 4:  Configure PC hosts.**

Refer to the Addressing Table for PC host address information.



**Part 2:   Create VLANs and Assign Switch Ports**

In Part 2, you will create VLANs as specified in the table above on both switches. You will then assign the VLANs to the appropriate interface and verify your configuration settings. Complete the following tasks on each switch.

**Step 1:  Create VLANs on both switches.**

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

*Open configuration window*

S1(config)# **vlan 10**

S1(config-vlan)# **name Management**

S1(config-vlan)# **vlan 20**

S1(config-vlan)# **name Sales**

S1(config-vlan)# **vlan 30**

S1(config-vlan)# **name Operations**

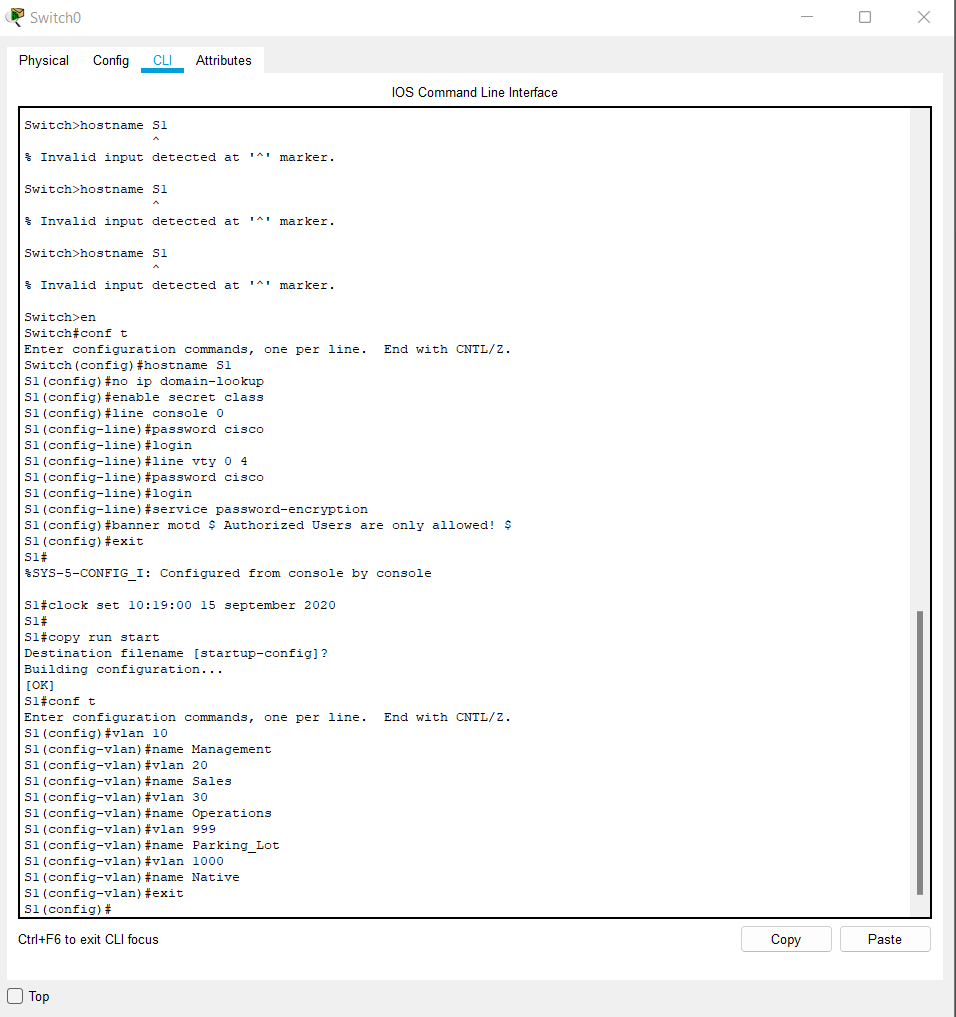
S1(config-vlan)# **vlan 999**

S1(config-vlan)# **name Parking\_Lot**

S1(config-vlan)# **vlan 1000**

S1(config-vlan)# **name Native**

S1(config-vlan)# **exit**



Same in switch s2

S2(config)# **vlan 10**

S2(config-vlan)# **name Management**

S2(config-vlan)# **vlan 20**

S2(config-vlan)# **name Sales**

S2(config-vlan)# **vlan 30**

S2(config-vlan)# **name Operations**

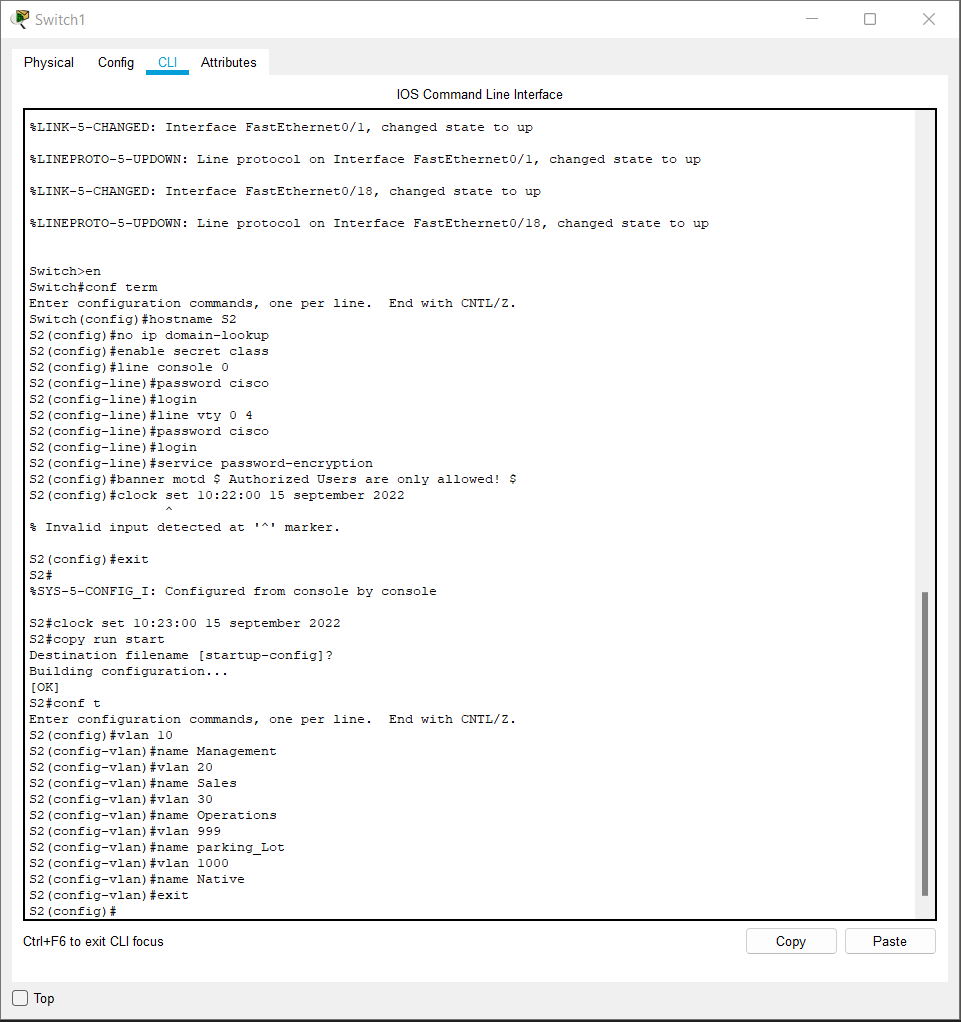
S2(config-vlan)# **vlan 999**

S2(config-vlan)# **name Parking\_Lot**

S2(config-vlan)# **vlan 1000**

S2(config-vlan)# **name Native**

S2(config-vlan)# **exit**



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

S1(config)# **interface vlan 10**

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

S1(config-if)# **no shutdown**

S1(config-if)# **exit**

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

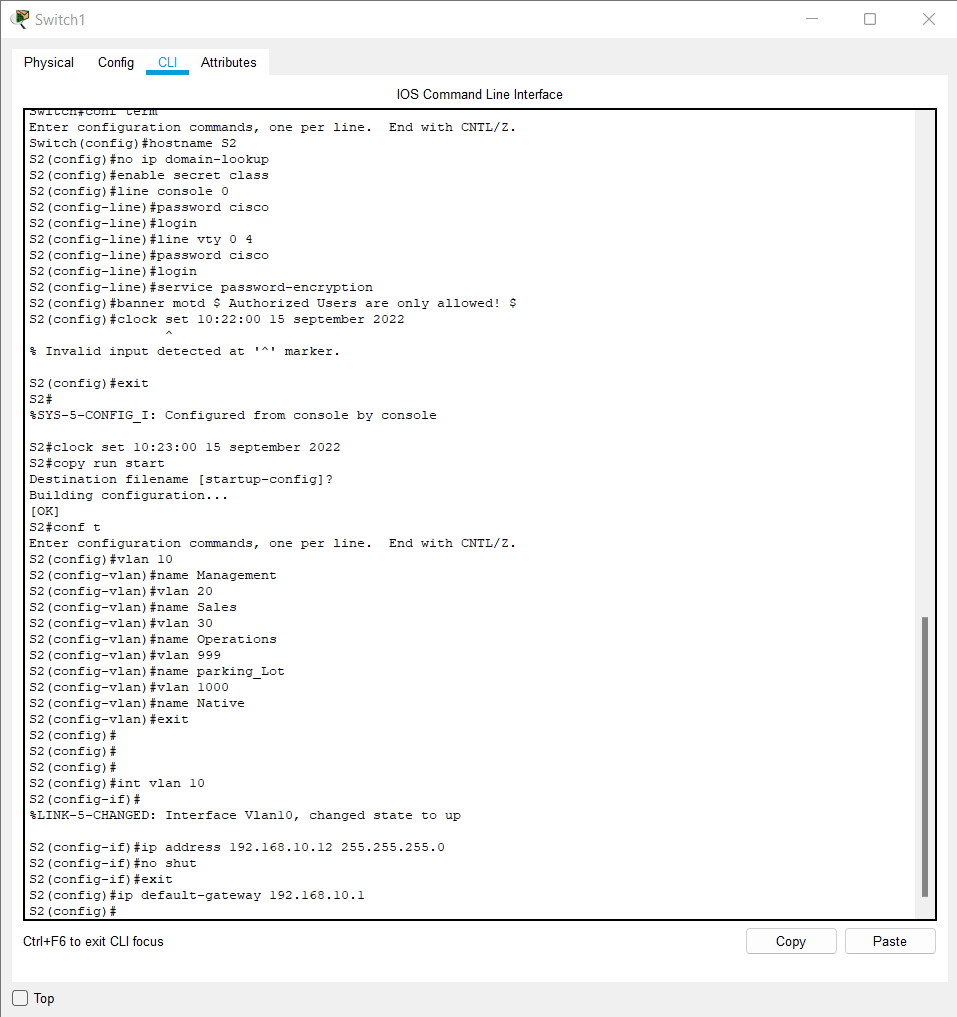
S2(config)# **interface vlan 10**

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

S2(config-if)# **no shutdown**

S2(config-if)# **exit**

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



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

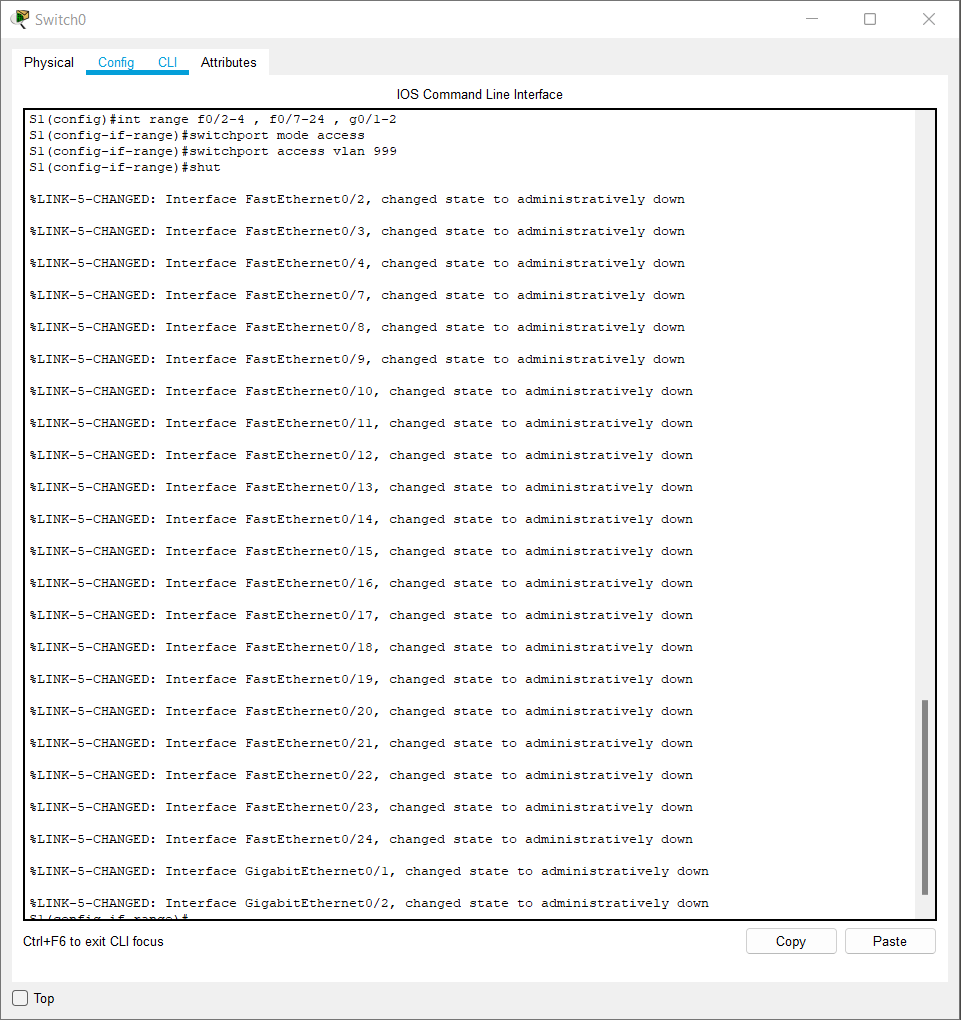
**Note**: The interface range command is helpful to accomplish this task with as few commands as necessary.

S1(config)#**interface range f0/2 – 4 , f0/7 – 24 , g0/1 – 2**

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

S1(config-if-range)# **switchport access vlan 999**

S1(config-if-range)# **shutdown**

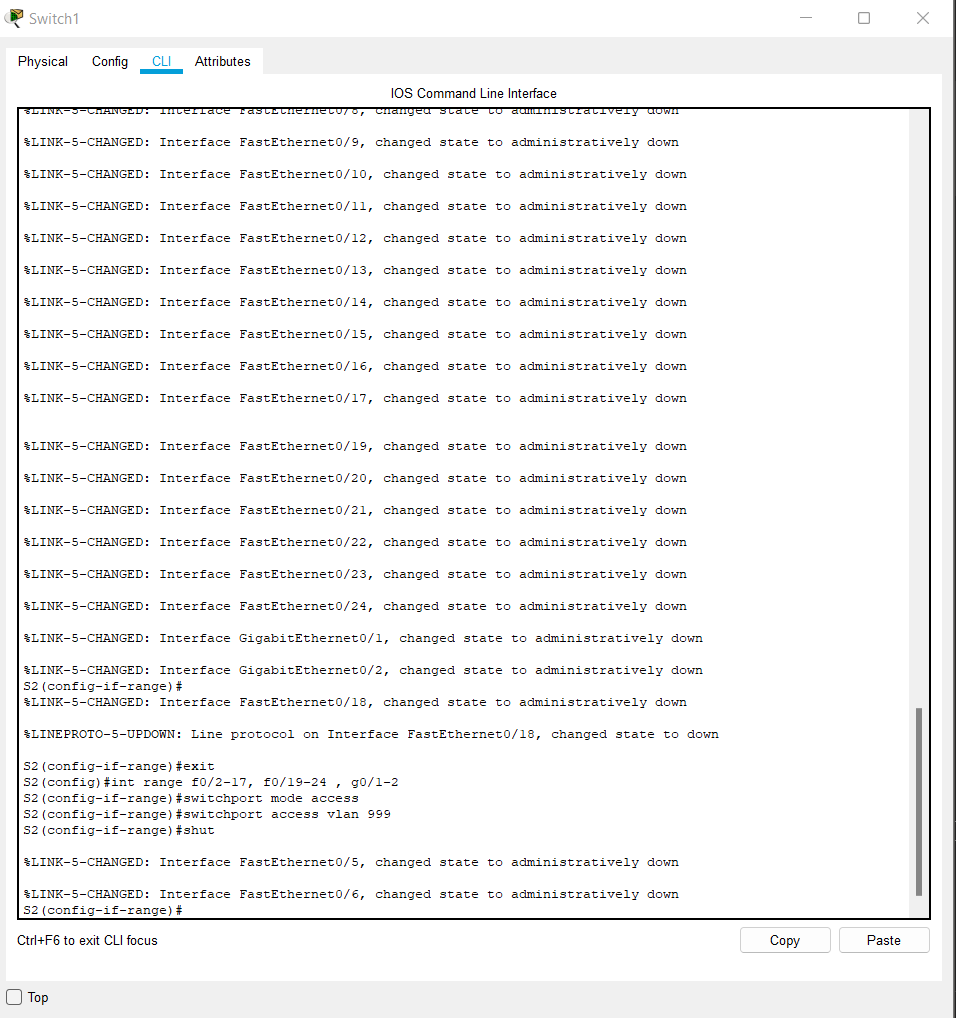


S2(config)#**interface range f0/2 – 17 , f0/19 – 24 , g0/1 – 2**

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

S2(config-if-range)# **switchport access vlan 999**

S2(config-if-range)# **shutdown**



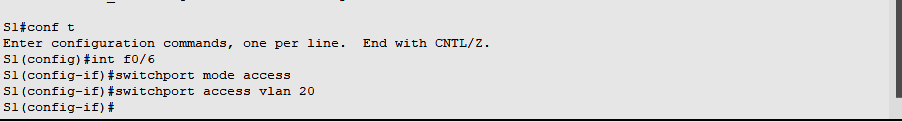
**Step 2:  Assign VLANs to the correct switch interfaces.**

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

S1(config)# **interface f0/6**

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

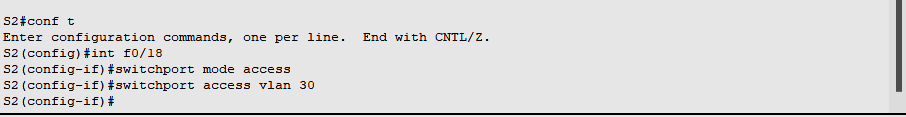
S1(config-if)# **switchport access vlan 20**



S2(config)# **interface f0/18**

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

S2(config-if)# **switchport access vlan** **30**



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

S1# **show vlan brief**

VLAN Name                             Status    Ports

—- ——————————– ——— ——————————-

1    default                          active    Fa0/1, Fa0/5

10   Management                       active

20   Sales                            active    Fa0/6

30   Operations                       active

999  Parking\_Lot                      active    Fa0/2, Fa0/3, Fa0/4, 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

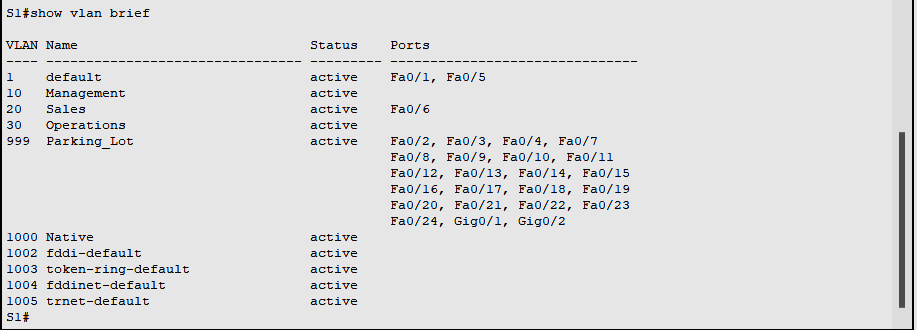
1000 Native                           active

1002 fddi-default                     act/unsup

1003 token-ring-default               act/unsup

1004 fddinet-default                  act/unsup

1005 trnet-default                    act/unsup



**S2# show vlan brief**

**VLAN Name                             Status    Ports**

**—- ——————————– ——— ——————————-**

**1    default                          active    Fa0/1**

**10   Management                       active**

**20   Sales                            active**

**30   Operations                       active    Fa0/18**

**999  Parking\_Lot                      active    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**

**Fa0/19, Fa0/20, Fa0/21, Fa0/22**

**Fa0/23, Fa0/24, Gi0/1, Gi0/2**

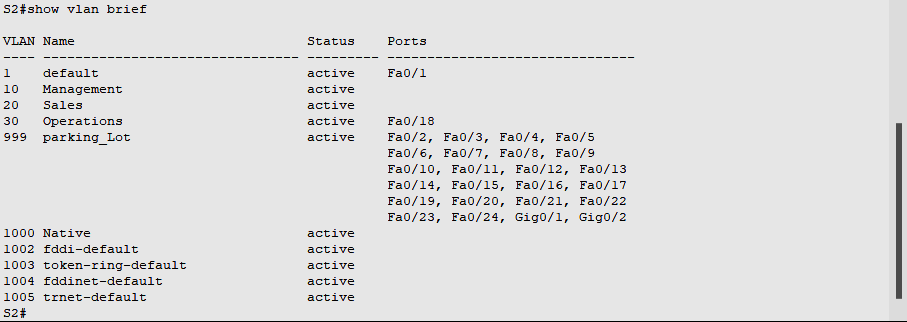
**1000 Native                           active**

**1002 fddi-default                     act/unsup**

**1003 token-ring-default               act/unsup**

**1004 fddinet-default                  act/unsup**

**1005 trnet-default                    act/unsup**



**Part 3:   Configure an 802.1Q Trunk Between the Switches**

In Part 3, you will manually configure interface F0/1 as a trunk.

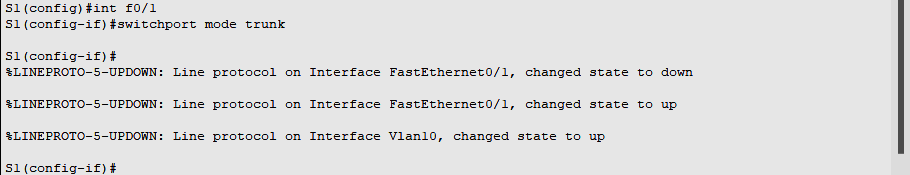
**Step 1:  Manually configure trunk interface F0/1 on switch S1 and S2.**

1. Configure static trunking on interface F0/1 for both switches.

*Open configuration window*

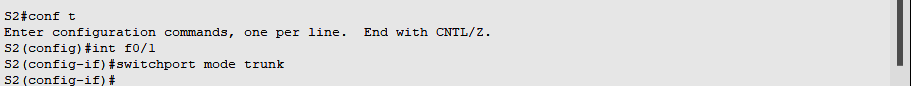
S1(config)# **interface f0/1**

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



S2(config)# **interface f0/1**

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



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

S1(config-if)# **switchport trunk native vlan 1000**

S2(config-if)# **switchport trunk native vlan 1000**

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

S1(config-if)# **switchport trunk allowed vlan 10,20,30,1000**

S2(config-if)# **switchport trunk allowed vlan 10,20,30,1000**

1. Verify trunking ports, the Native VLAN and allowed VLANs across the trunk.

S1# **show interfaces trunk**

Port        Mode             Encapsulation  Status        Native vlan

Fa0/1       on               802.1q         trunking      1000

Port        Vlans allowed on trunk

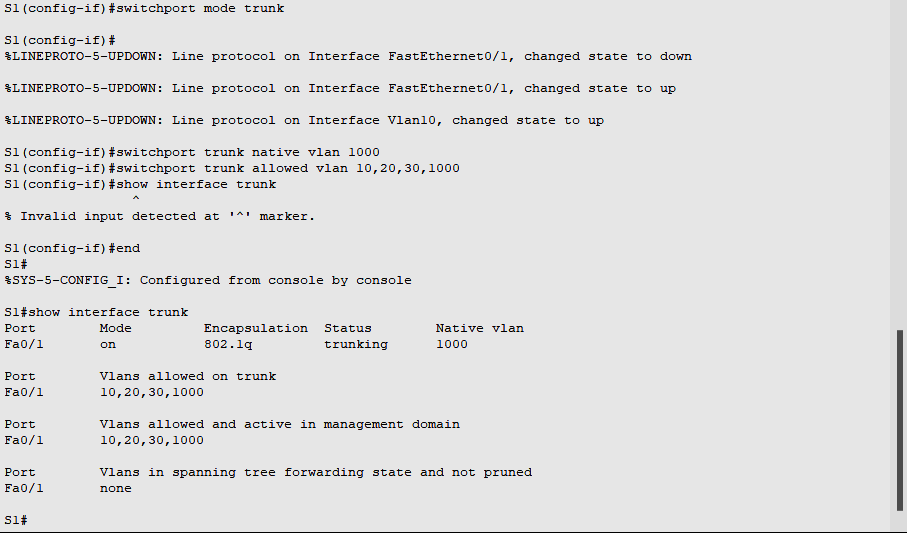
Fa0/1       10,20,30,1000

Port        Vlans allowed and active in management domain

Fa0/1       10,20,30,1000

Port        Vlans in spanning tree forwarding state and not pruned

Fa0/1       10,20,30,1000



S2# **show interfaces trunk**

Port        Mode             Encapsulation  Status        Native vlan

Fa0/1       on               802.1q         trunking      1000

Port        Vlans allowed on trunk

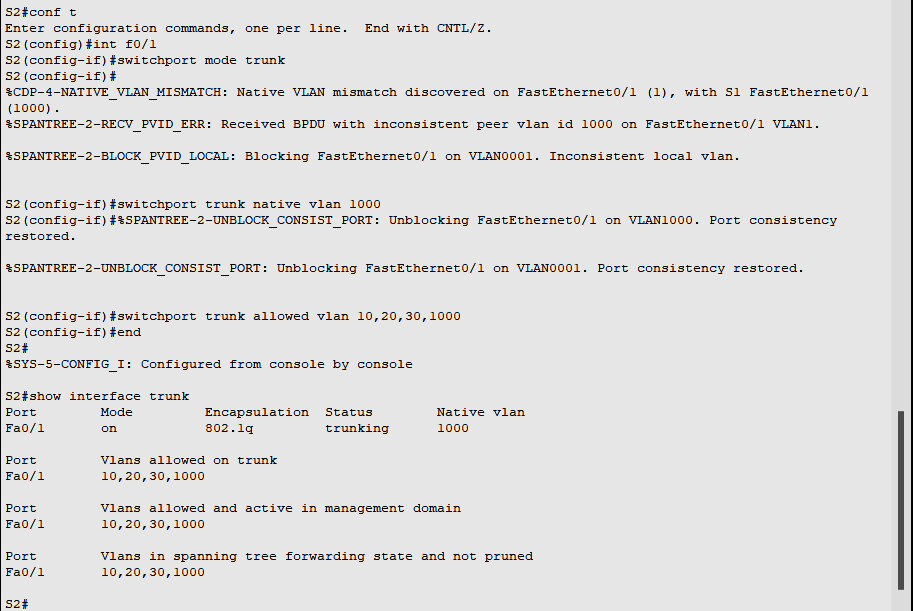
Fa0/1       10,20,30,1000

Port        Vlans allowed and active in management domain

Fa0/1       10,20,30,1000

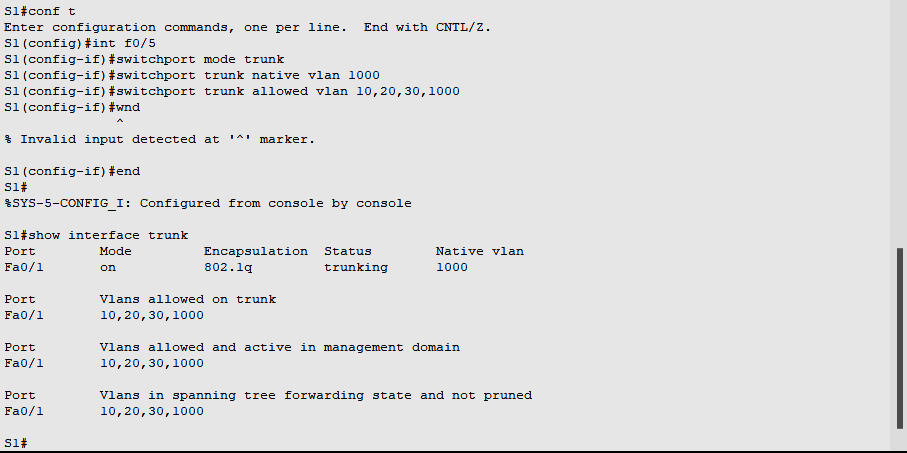
Port        Vlans in spanning tree forwarding state and not pruned

Fa0/1       10,20,30,1000



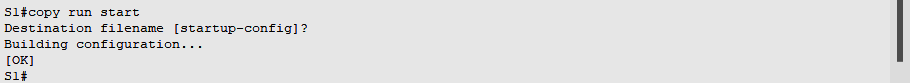
**Step 2:  Manually configure S1’s trunk interface F0/5**

1. Configure S1’s interface F0/5 with the same trunk parameters as F0/1. This is the trunk to the router.

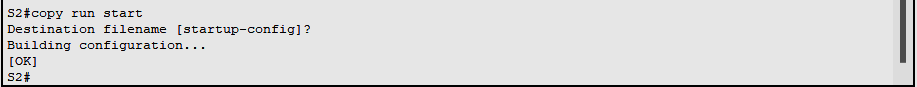


1. Save the running configuration to the startup configuration file.

S1# **copy running-config startup-config**



S2# **copy running-config startup-config**



1. Verify trunking.

Question:

What happens if G0/0/1 on R1 is down?

**S1 F0/5 will not be displayed if the GigabitEthernet 0/0/1 interface status on the router is down.**

**Part 4:   Configure Inter-VLAN Routing on the Router**

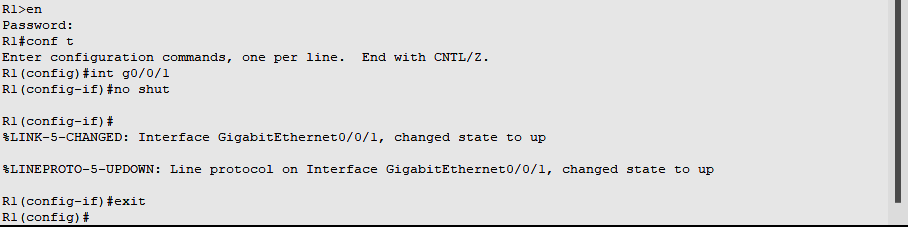
**Step 1:  Configure the router.**

Activate interface G0/0/1 as necessary on the router.

R1(config)# **interface g0/0/1**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**



1. 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 g0/0/1.10**

R1(config-subif)# **description Management Network**

R1(config-subif)# **encapsulation dot1q 10**

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

R1(config-subif)# **interface g0/0/1.20**

R1(config-subif)# **encapsulation dot1q 20**

R1(config-subif)# **description Sales Network**

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

R1(config-subif)# **interface g0/0/1.30**

R1(config-subif)# **encapsulation dot1q 30**

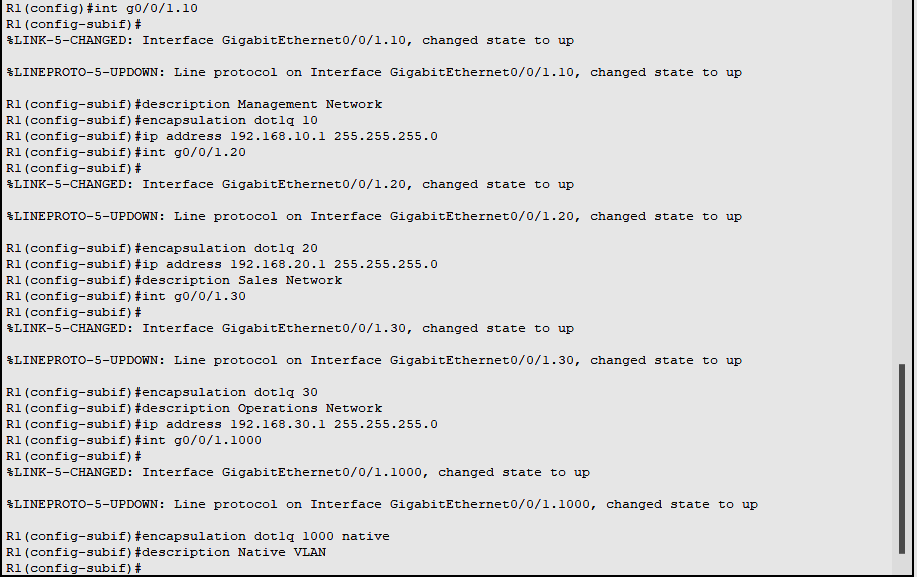
R1(config-subif)# **description Operations Network**

R1(config-subif)# **ip address 192.168.30.1 255.255.255.0**

R1(config-subif)# **interface g0/0/1.1000**

R1(config-subif)# **encapsulation dot1q 1000 native**

R1(config-subif)# **description Native VLAN**



1. Verify the sub-interfaces are operational

R1# **show ip interface brief**

Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down

GigabitEthernet0/0/1   unassigned      YES NVRAM  up                    up

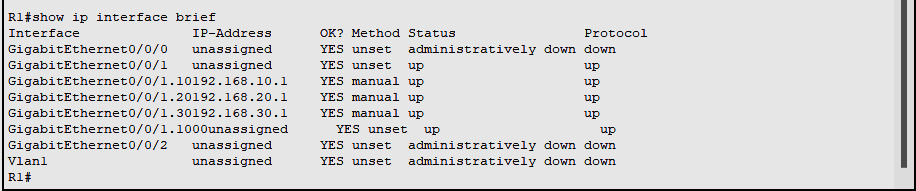
Gi0/0/1.10             192.168.10.1    YES manual up                    up

Gi0/0/1.20             192.168.20.1    YES manual up                    up

Gi0/0/1.30             192.168.30.1    YES manual up                    up

Gi0/0/1.1000           unassigned      YES unset  up                    up

GigabitEthernet0       unassigned      YES NVRAM  down                  down

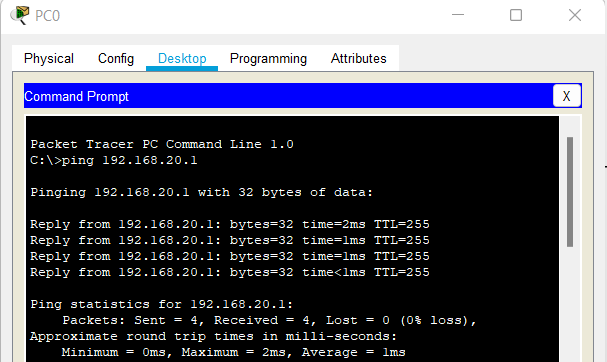


**Part 5:   Verify Inter-VLAN Routing is Working**

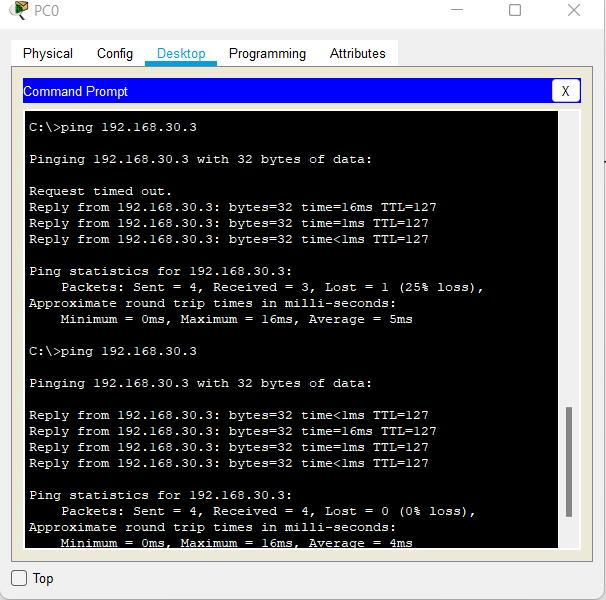
**Step 1:  Complete the following tests from PC-A. All should be successful.**

**Note:** You may have to disable the PC firewall for pings to work

1. Ping from PC-A to its default gateway. 192.168.20.1



1. Ping from PC-A to PC-B



1. Ping from PC-A to S2

