**INDEX**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr .No.** | **Practicals** | Page no | Sign |
| 1 | Implement IP SLA (IP Service Level Agreement) |  |  |
| 2 | Implement IPv4 ACLs   1. Standard 2. Extended |  |  |
| 3 | 1. Implement SPAN Technologies (Switch Port Analyzer) 2. Implement SNMP and Syslog 3. Implement Flexible NetFlow |  |  |
| 4 | 1. Implement a GRE Tunnel 2. Implement VTP 3. Implement NAT |  |  |
| 5 | Implement Inter-VLAN Routing |  |  |

# Practical no.1

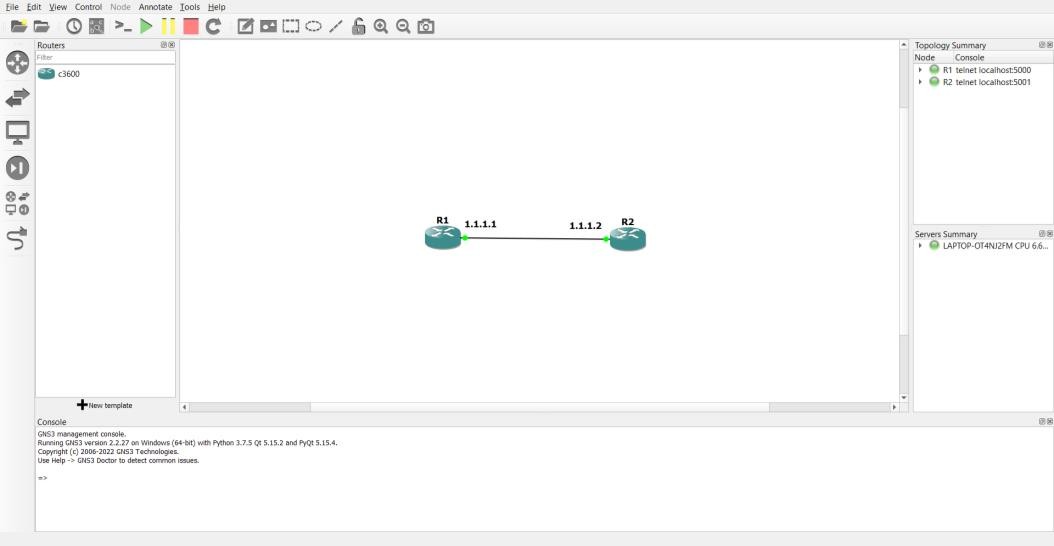
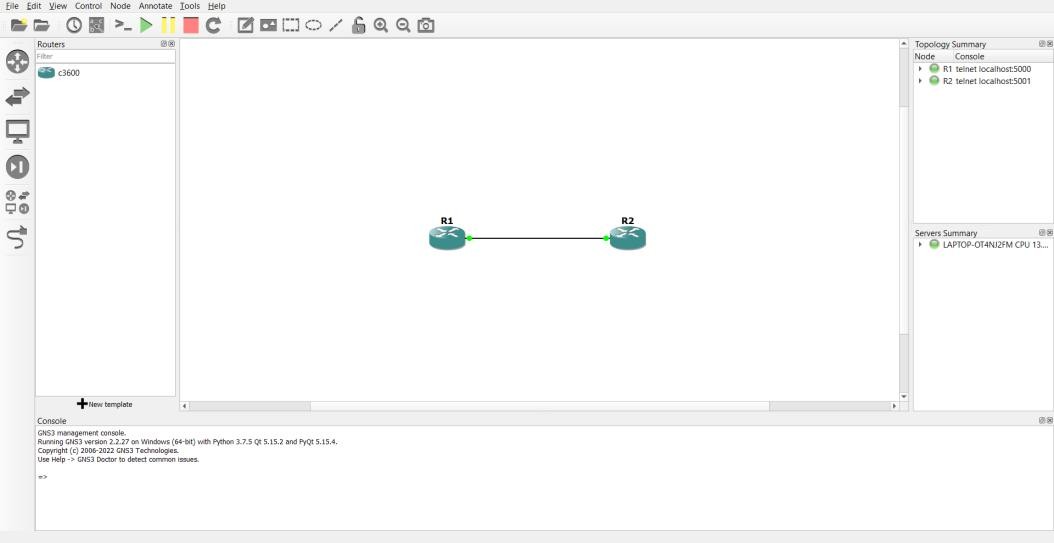
## Implement IP SLA (IP Service Level Agreement)

**Aim:** To implement IP SLA (IP Service Level Agreement) using GNS3 tool.

**Requirement:** GNS3 tool.

### Procedure:

**Step1: Build the Network.**



### Step 2: Configure Routers:

* **Configure Router R2:**

### Input:

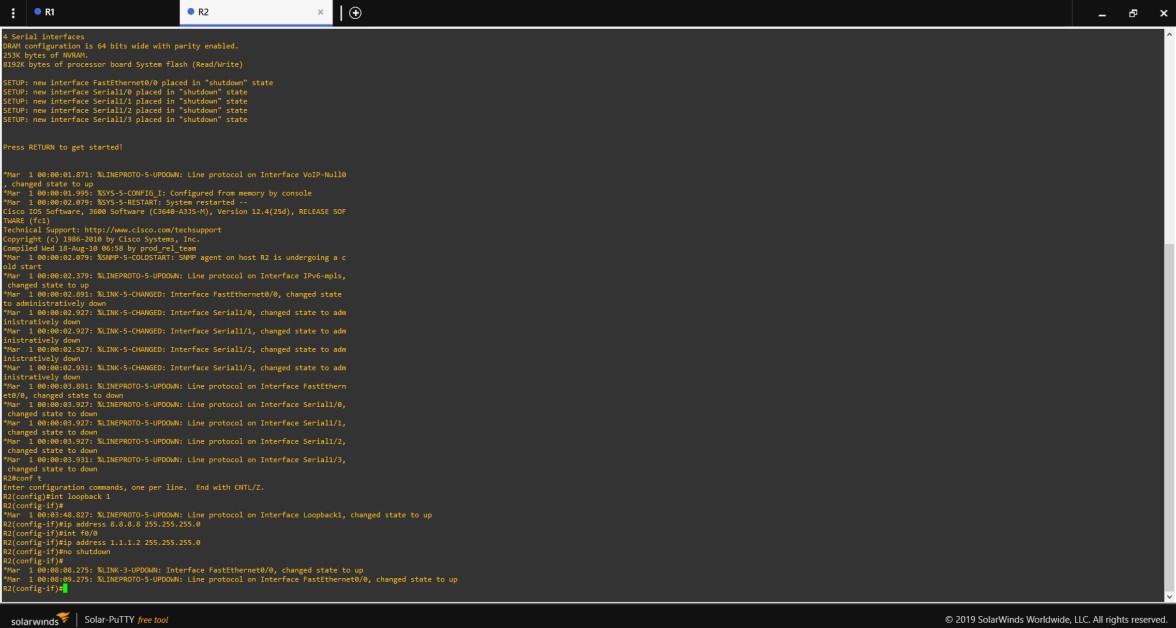
R2#conf t

R2(config)#int loopback 1

R2(config-if)#ip address 8.8.8.8 255.255.255.0 R2(config-if)#int f0/0

R2(config-if)#ip address 1.1.1.2 255.255.255.0 R2(config-if)#no shutdown

### Output:



* **Configure Router R1: Input:**

R1#conf t R1(config)#int f0/0

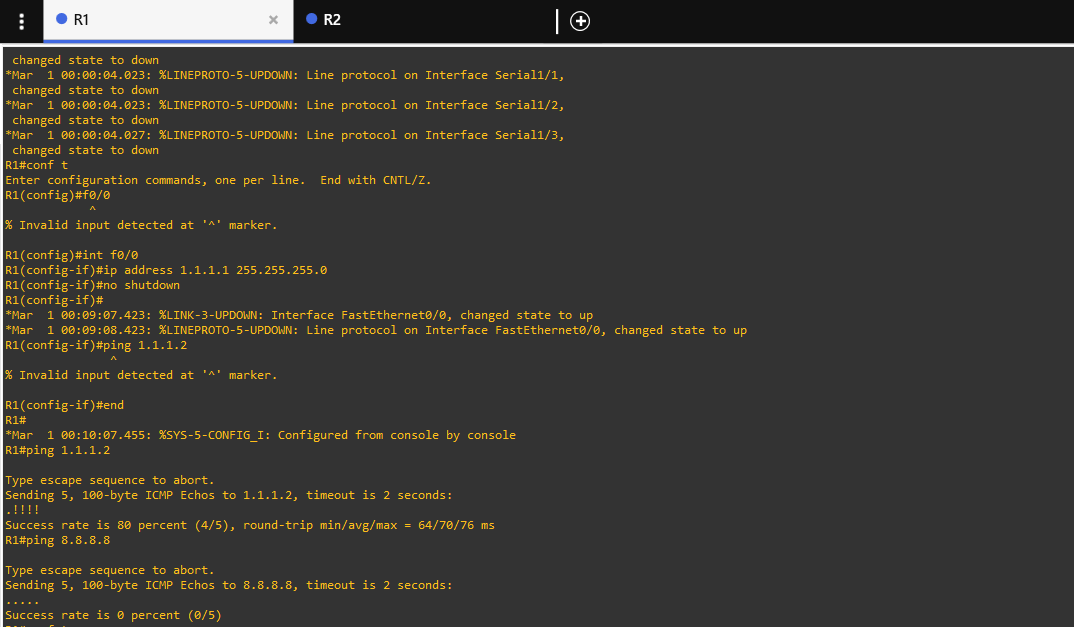
R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#no shutdown R1(config-if)#end

R1#ping 1.1.1.2

R1#ping 8.8.8.8

### Output:



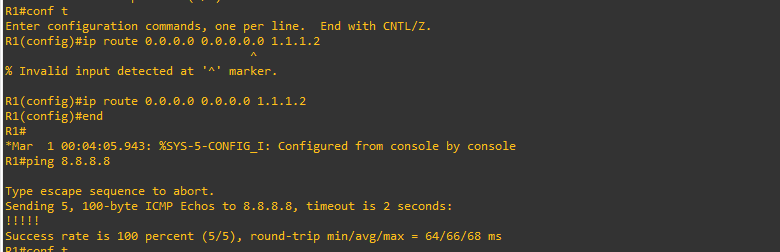
**Input:**

R1#conf t

R1(config)#ip route 0.0.0.0 0.0.0.0.0 1.1.1.2 R1(config)#end

R1#ping 8.8.8.8

### Output:



**Input:**

R1(config)#ip sla monitor 1

R1(config-sla-monitor)#$rotocol ipIcmpEcho 8.8.8.8 source-ipaddr 1.1.1.1

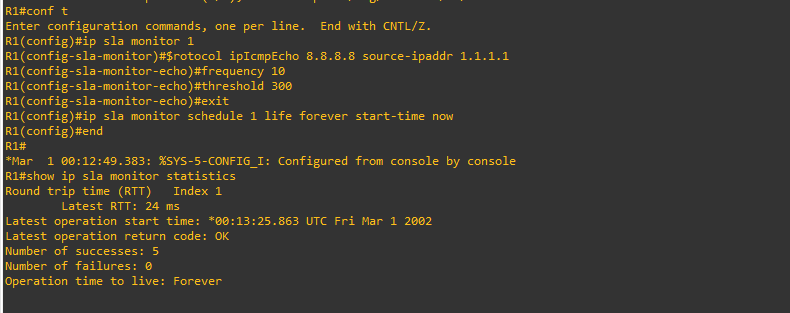
R1(config-sla-monitor-echo)#frequency 10

R1(config-sla-monitor-echo)#threshold 300 R1(config-sla-monitor-echo)#exit

R1(config)#ip sla monitor schedule 1 life forever start-time now R1(config)#end

R1#show ip sla monitor statistics R1#debug ip icmp

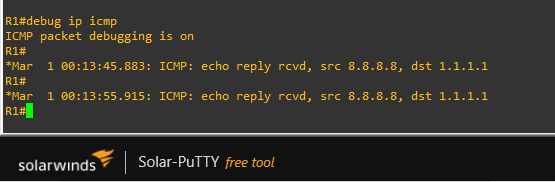
### Output:



Note:-

To stop debug use this or at some point memory will get full. R1#undebug all

# Output:



Practical no.5

## Implement Inter-VLAN Routing

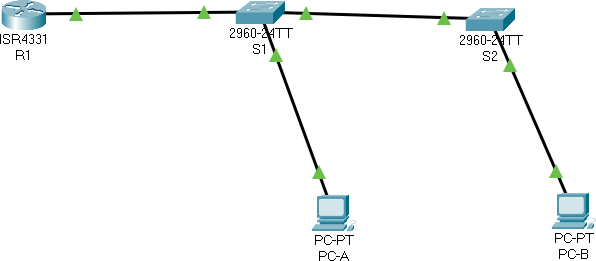
**Aim:** To implement Inter-VLAN Routing using Cisco Packet Tracer.

**Requirement:** Cisco Packet Tracer tool.

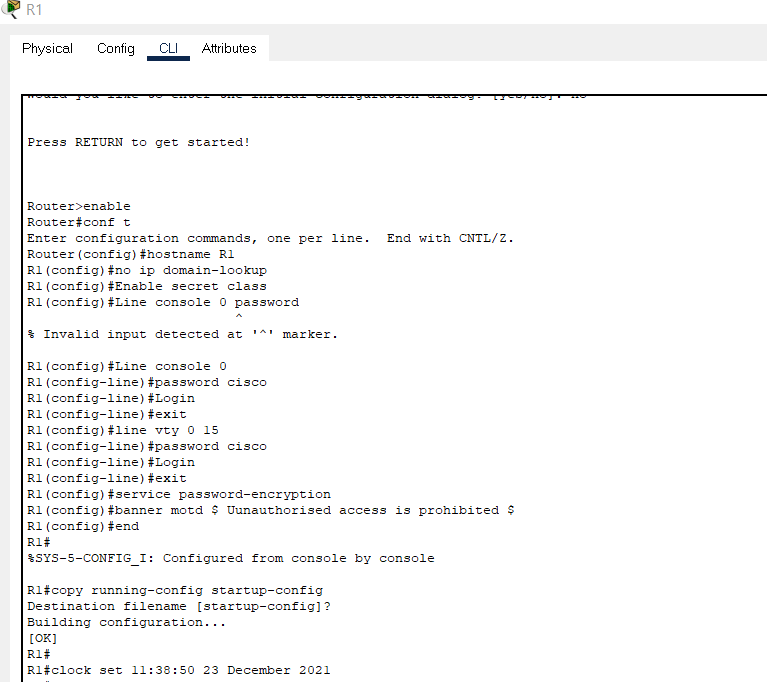
### Procedure:

**Part 1:**

**Step1: Build the Network and Configure Basic Device Settings:**



**Output:**



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

1. Console into the router and enable privileged EXEC mode. router> enable
2. Enter configuration mode. router# conf t
3. Assign a device name to the router. router(config)# hostname R1
4. 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

1. Assign class as the privileged EXEC encrypted password. R1(config)# enable secret class
2. Assign cisco as the console password and enable login. R1(config)# line console 0

R1(config-line)# password cisco R1(config-line)# login

1. Assign cisco as the vty password and enable login. R1(config)# line vty 0 15

R1(config-line)# password cisco R1(config-line)# login

1. Encrypt the plaintext passwords. R1(config)# service password-encryption
2. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

R1(config)# banner motd $ Unauthorised access is prohibited $ 10.Save the running configuration to the startup configuration file.

R1(config)# end

R1# copy running-config startup-config 11.Set the clock on the router.

R1# clock set 11:38:50 23 December 2021

### Step 3: Configure basic settings for switch 1.

1. Assign a device name to the switch. switch(config)# hostname S1
2. 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

1. Assign class as the privileged EXEC encrypted password. S1(config)# enable secret class
2. Assign cisco as the console password and enable login. S1(config)# line console 0

S1(config-line)# password cisco S1(config-line)# login

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

1. Encrypt the plaintext passwords. S1(config)# service password-encryption
2. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# banner motd “Unauthorised access is prohibited” S2(config)# exit

1. Set the clock on the switch.

S1# clock set 11:48:10 23 December 2021

1. Save the running configuration to the startup configuration. S1# copy run st

### Output:

**Configure basic settings for Switch 2:**

* 1. Assign a device name to the switch. switch(config)# hostname S2
  2. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

S2(config)# no ip domain-lookup

* 1. Assign class as the privileged EXEC encrypted password. S2(config)# enable secret class
  2. Assign cisco as the console password and enable 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. S2(config)# line vty 0 15

S2(config-line)# password cisco S2(config-line)# login

* 1. Encrypt the plaintext passwords. S2(config)# service password-encryption
  2. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S2(config)# banner motd “Unauthorised access is prohibited” S2(config)# exit

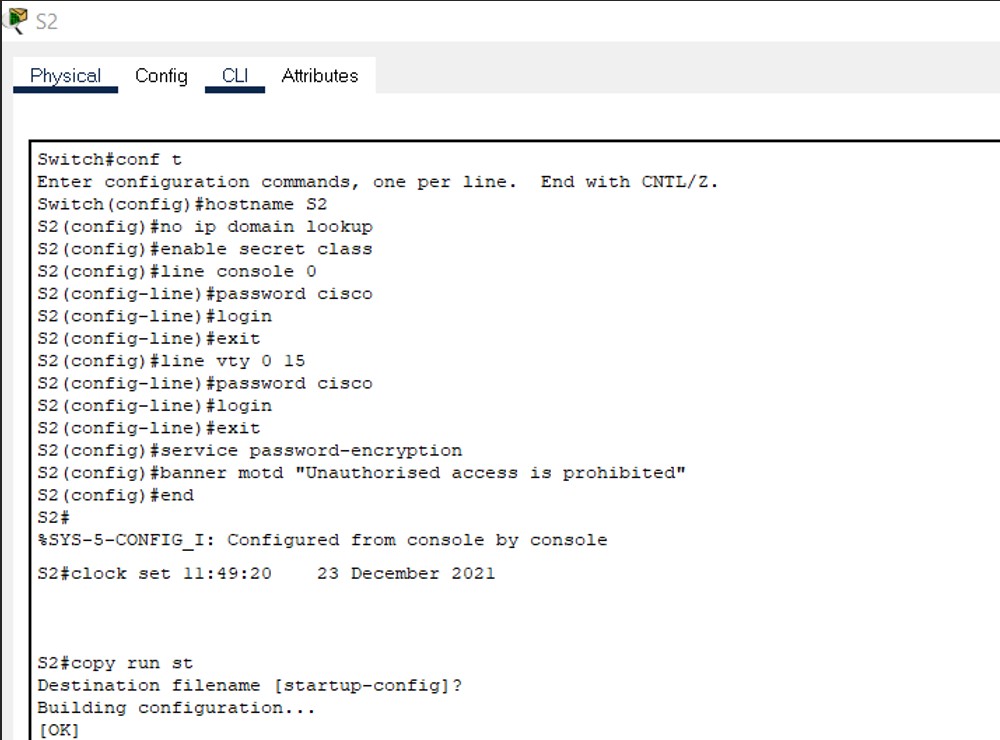
* 1. Set the clock on the switch.

S2# clock set 11:49:20 23 December 2021

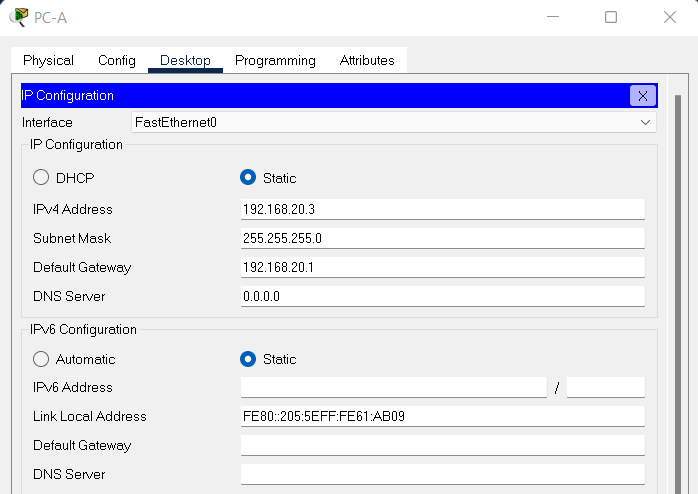
* 1. Save the running configuration to the startup configuration.

S2# copy run st

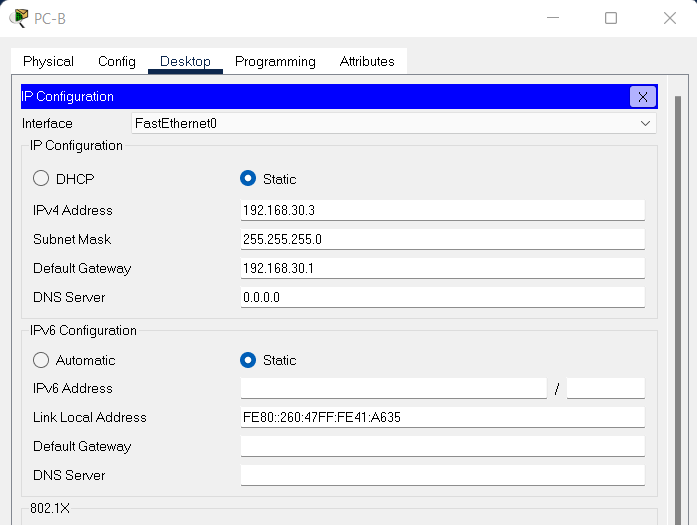
### Output:



**Step 4: Configure PC hosts.** **PC-A:**



### PC-B:



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

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

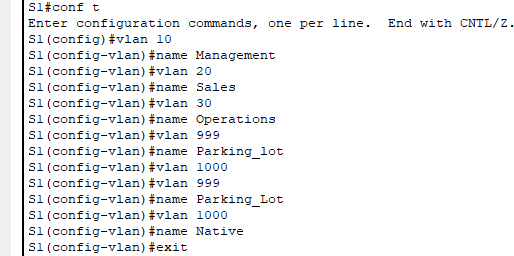
1. Create and name the required VLANs on each switch from the table above.

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

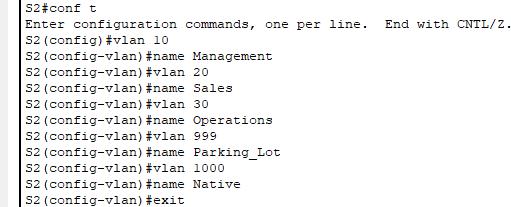


S2(config)# vlan 10

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



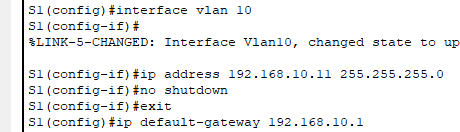
1. Configure the management interface and default gateway on each switch using the IP address information in the Addressing Table.

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

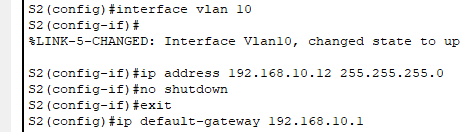


S2(config)# interface vlan 10

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

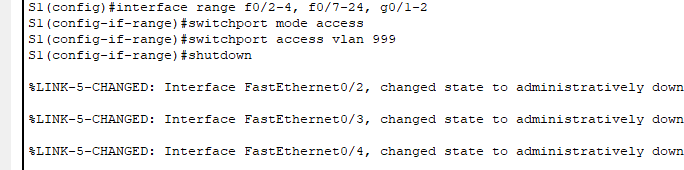


1. Assign all unused ports on the switch to the Parking\_Lot VLAN, configure them for static access mode, and administratively deactivate them.

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

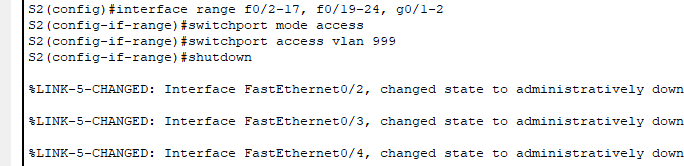
S1(config)# interface range f0/2 – 4 , f0/7 – 24 , g0/1 – 2

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**

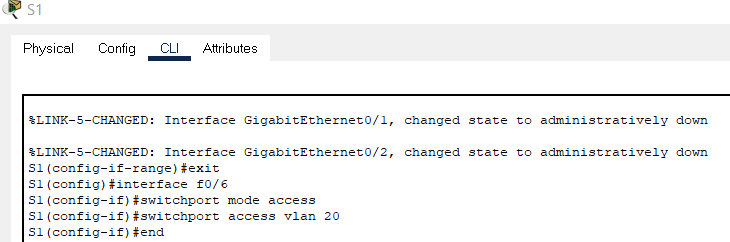


### Step 2: Assign VLANs to the correct switch interfaces.

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

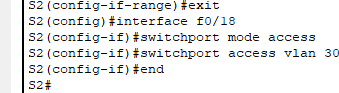
S1(config)# interface f0/6

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

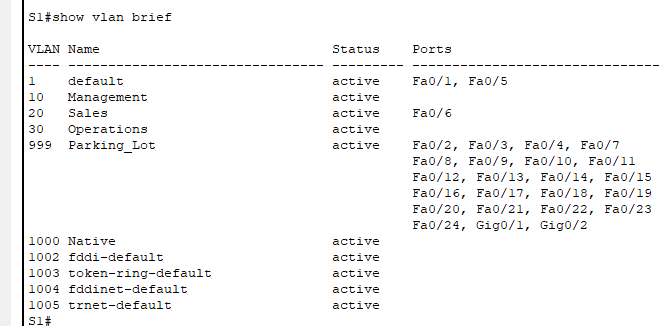


S2(config)# interface f0/18

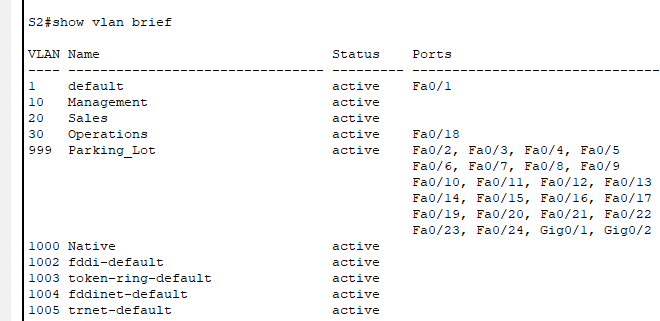
S2(config-if)# switchport mode access S2(config-if)# switchport access vlan 30



1. Verify that the VLANs are assigned to the correct interfaces. S1# show vlan brief



S2# show vlan brief



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

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

1. Configure static trunking on interface F0/1 for both switches. S1(config)# interface f0/1

S1(config-if)# switchport mode trunk

1. Set the native VLAN to 1000 on both switches. S1(config-if)# switchport trunk native vlan 1000
2. 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
3. Verify trunking ports, the Native VLAN and allowed VLANs across the trunk.

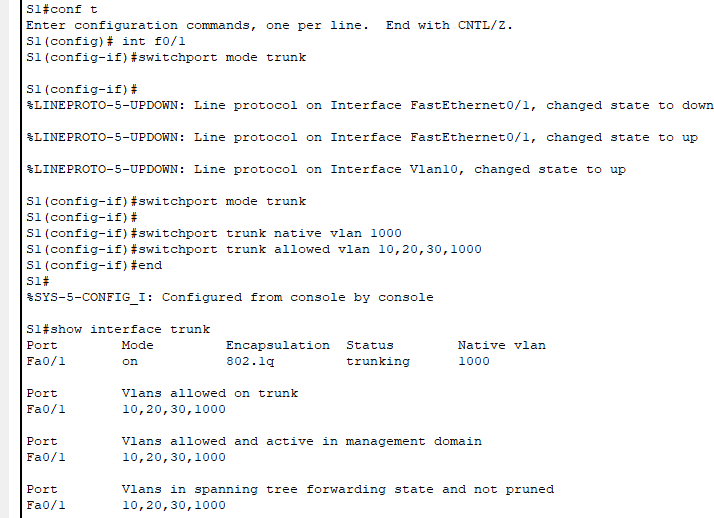
S1# show interfaces trunk

|  |  |  |  |
| --- | --- | --- | --- |
| 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



### Switch 2:

1. Configure static trunking on interface F0/1 for both switches. S2(config)# interface f0/1

S2(config-if)# switchport mode trunk

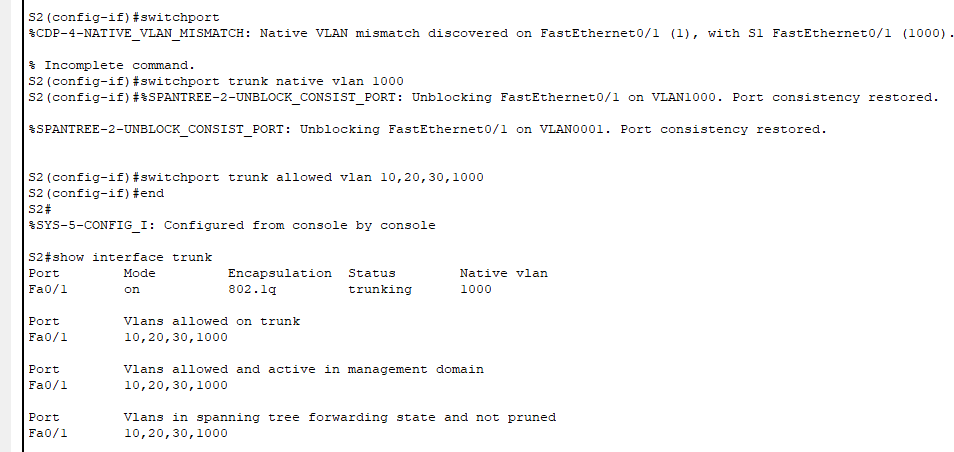
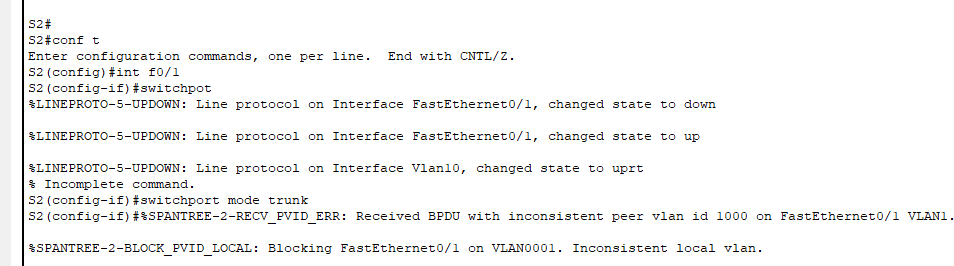
1. Set the native VLAN to 1000 on both switches. S2(config-if)# switchport trunk native vlan 1000
2. Specify that VLANs 10, 20, 30, and 1000 are allowed to cross the trunk. S2(config-if)# switchport trunk allowed vlan 10,20,30,1000
3. Verify trunking ports, the Native VLAN and allowed VLANs across the trunk.

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

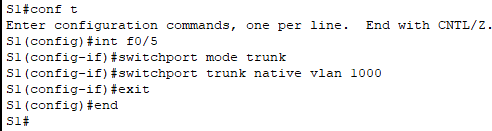
Port Vlans allowed and active in management domain Fa0/1 10,20,30,1000

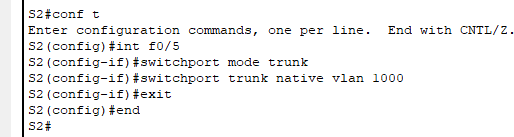


Port Vlans in spanning tree forwarding state and not pruned Fa0/1 10,20,30,1000

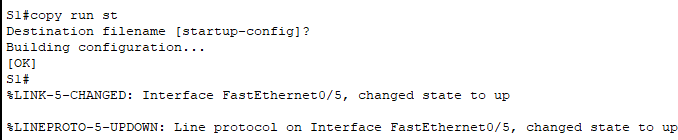
### Step 2: Manually configure S1’s trunk interface F0/5

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

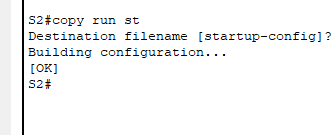
Switch 1:

Switch 2:

1. Save the running configuration to the startup configuration file. S1# **copy run st**



S2# **copy run st**



1. Verify trunking.

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.

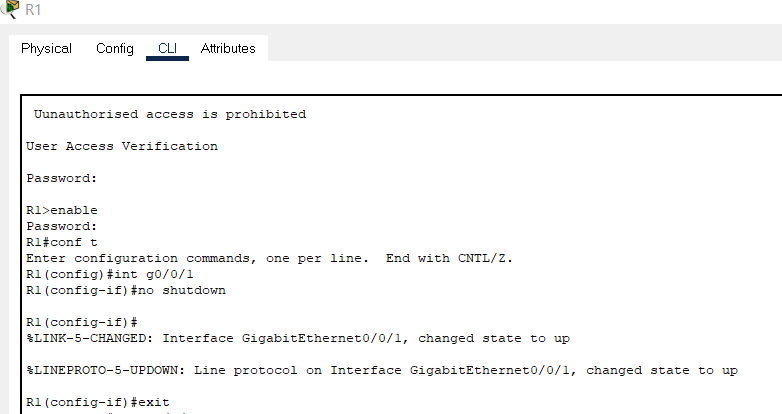
### Part 4: Configure Inter-VLAN Routing on the Router

**Step 1: Configure the router.**

*Open configuration window*

1. 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

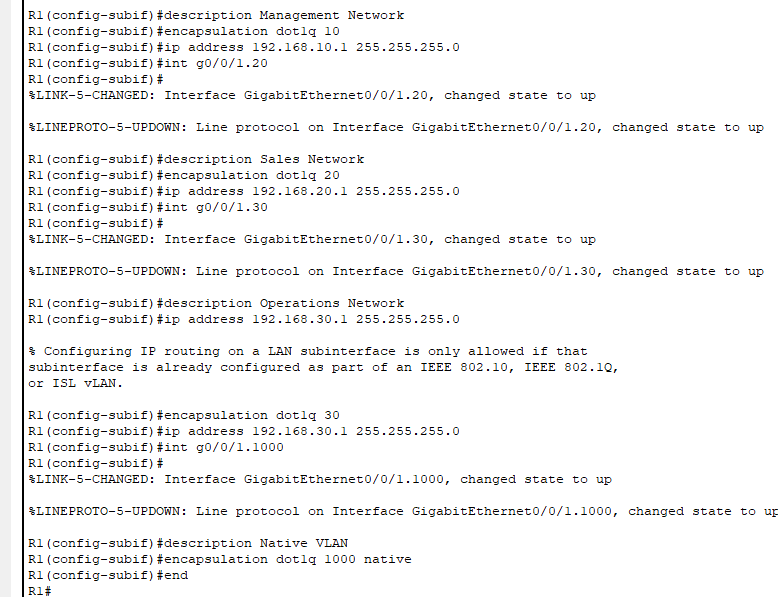
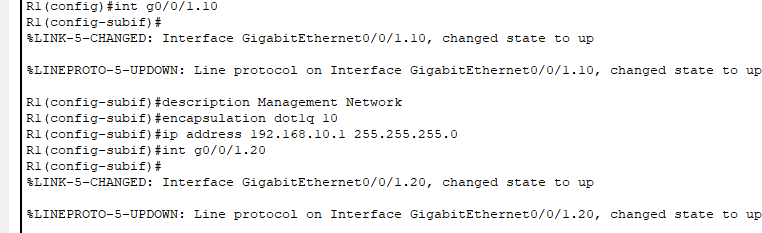
R1(config-subif)# description Management Network R1(config-subif)# encapsulation dot1q 10

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

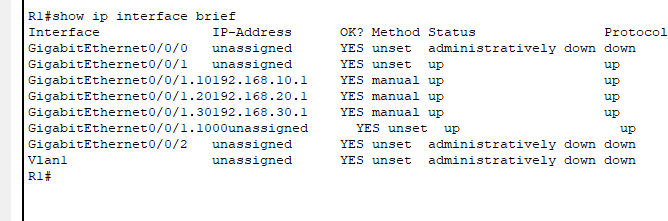


R1(config-subif)# ip address 192.168.30.1 255.255.255.0 R1(config-subif)# interface g0/0/1.1000

R1(config-subif)# encapsulation dot1q 1000 native R1(config-subif)# description Native VLAN

Output:

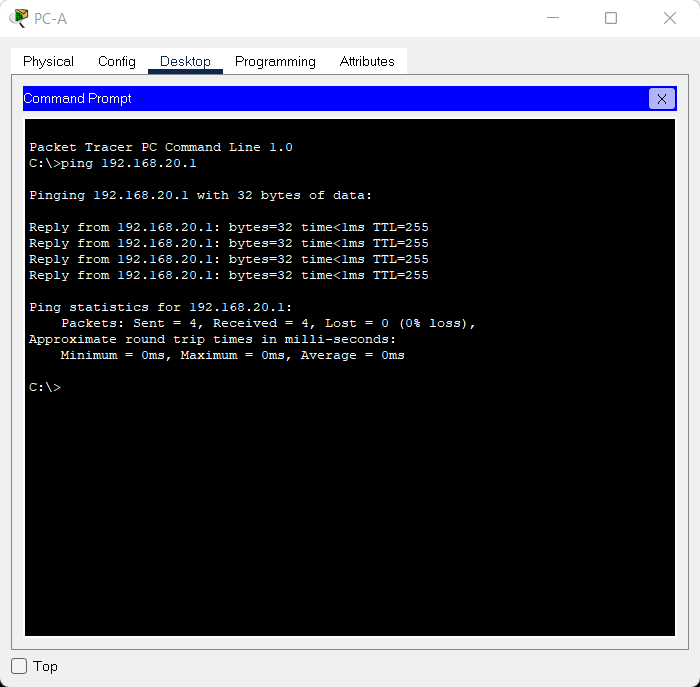
3). Verify the sub-interfaces are operational R1# show ip interface brief



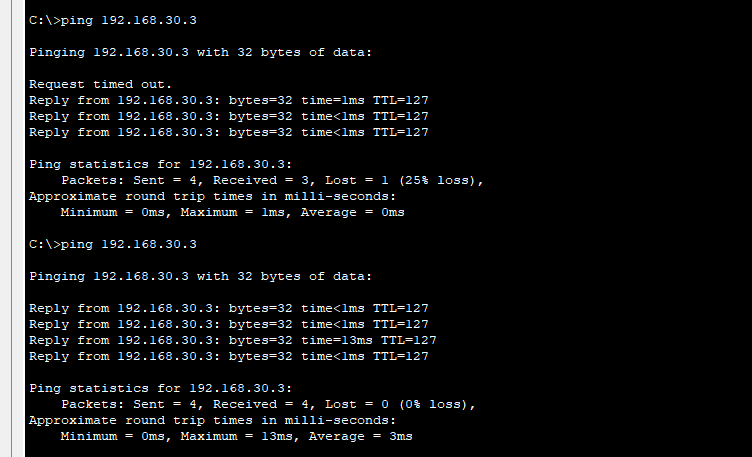
### Part 5: Verify Inter-VLAN Routing is Working

**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 OUTPUT:-**

### Ping from PC-A to PC-B Output:



1. **Ping from PC-A to S2**

### Step 2: Complete the following test from PC-B.

**From the Command Prompt window on PC-B, issue the tracert command to the address of PC-A.**:

### Output:

