

INDEX

Sr .No.	TOPICS
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

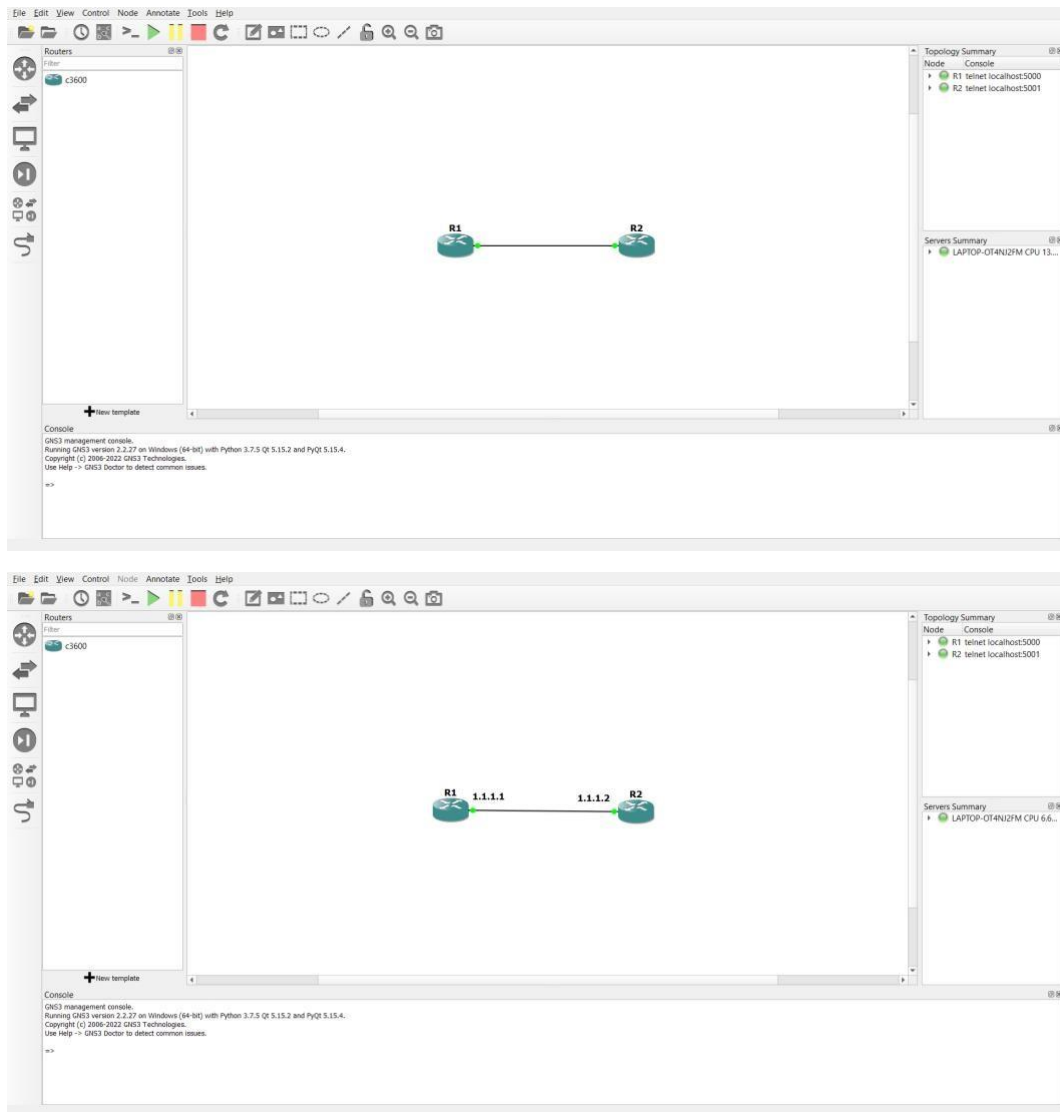
Implement IP SLA (IP Service Level Agreement)

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:

```

R1 R2
Serial Interface
DHAP configuration is 64 bits wide with parity enabled.
25Kc bytes of RAM.
1024Kc bytes of processor board System Flash (Read/Write)

SETUP: new Interface FastEthernet0/0 placed in "shutdown" state
SETUP: new Interface Serial1/0 placed in "shutdown" state
SETUP: new Interface Serial2/1 placed in "shutdown" state
SETUP: new Interface Serial1/2 placed in "shutdown" state
SETUP: new Interface Serial1/3 placed in "shutdown" state

Press RETURN to get started!

Mar 1 00:00:00.871: NLINKPROTO-S-UPDOWN: Line protocol on Interface VSP-Mull0
changed state to up
Mar 1 00:00:01.991: XSYS-S-COMP[R]: Configured from memory by console
Mar 1 00:00:02.079: XSYS-S-RESTART: System restarted --
Cisco IOS Software, 3600 Software (C3600-AD33-M), Version 12.4(24d), RELEASE SGP
TAAAR (fc)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled 18-Aug-10 06:18 by prod_rel_team
Mar 1 00:00:02.079: XSYS-S-STATUS: New agent on host R2 is undergoing a c
old start
Mar 1 00:00:02.379: NLINKPROTO-S-UPDOWN: Line protocol on Interface IPd-mpl0
changed state to up
Mar 1 00:00:02.891: NLINK-S-CHANGED: Interface FastEthernet0/0, changed sta
administratively down
Mar 1 00:00:02.927: NLINK-S-CHANGED: Interface Serial1/0, changed state to ad
ministratively down
Mar 1 00:00:02.927: NLINK-S-CHANGED: Interface Serial1/1, changed state to ad
ministratively down
Mar 1 00:00:02.927: NLINK-S-CHANGED: Interface Serial1/2, changed state to ad
ministratively down
Mar 1 00:00:02.931: NLINK-S-CHANGED: Interface Serial1/3, changed state to ad
ministratively down
Mar 1 00:00:03.011: NLINKPROTO-S-UPDOWN: Line protocol on Interface FastEth
ernet0/0, changed state to down
Mar 1 00:00:03.927: NLINKPROTO-S-UPDOWN: Line protocol on Interface Serial1/0
changed state to down
Mar 1 00:00:03.927: NLINKPROTO-S-UPDOWN: Line protocol on Interface Serial1/1
changed state to down
Mar 1 00:00:03.927: NLINKPROTO-S-UPDOWN: Line protocol on Interface Serial1/2
changed state to down
Mar 1 00:00:03.931: NLINKPROTO-S-UPDOWN: Line protocol on Interface Serial1/3
changed state to down
Mar 1 00:00:03.931: NLINKPROTO-S-UPDOWN: Line protocol on Interface Serial1/3
changed state to down
Mar 1 00:00:04.011: NLINKPROTO-S-UPDOWN: Line protocol on Interface Serial1/3
changed state to down
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int loopback1
R1(config-if)#
Mar 1 00:01:48.837: NLINK-S-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R1(config-if)#ip address 8.8.8.8 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#
Mar 1 00:01:49.275: NLINK-S-UPDOWN: Interface FastEthernet0/0, changed state to up
Mar 1 00:01:49.275: NLINK-S-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#

```

- **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:

```

R1
R2
changed state to down
*Mar 1 00:00:04.023: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1,
changed state to down
*Mar 1 00:00:04.023: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2,
changed state to down
*Mar 1 00:00:04.027: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/3,
changed state to down
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#f0/0
^
% Invalid input detected at '^' marker.

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)#
*Mar 1 00:09:07.423: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:09:08.423: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#ping 1.1.1.2
^
% Invalid input detected at '^' marker.

R1(config-if)#end
R1#
*Mar 1 00:10:07.455: %SYS-5-CONFIG_I: Configured from console by console
R1#ping 1.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 64/70/76 ms
R1#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Input:

R1#conf t

R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2

R1(config)#end

R1#ping 8.8.8.8

Output:

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
^
% Invalid input detected at '^' marker.

R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
R1(config)#end
R1#
*Mar 1 00:04:05.943: %SYS-5-CONFIG_I: Configured from console by console
R1#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/66/68 ms
R1#conf t
```

Input:

```
R1(config)#ip sla monitor 1
R1(config-sla-monitor)#$protocol 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:

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip sla monitor 1
R1(config-sla-monitor)#$protocol 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#
*Mar  1 00:12:49.383: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip sla monitor statistics
Round trip time (RTT)    Index 1
      Latest RTT: 24 ms
Latest operation start time: *00:13:25.863 UTC Fri Mar 1 2002
Latest operation return code: OK
Number of successes: 5
Number of failures: 0
Operation time to live: Forever
```


Note:-

To stop debug use this or at some point memory will get full.

```
R1#undebug all
```

Output:

```
R1#debug ip icmp
ICMP packet debugging is on
R1#
*Mar  1 00:13:45.883: ICMP: echo reply rcvd, src 8.8.8.8, dst 1.1.1.1
R1#
*Mar  1 00:13:55.915: ICMP: echo reply rcvd, src 8.8.8.8, dst 1.1.1.1
R1#
```

solarwinds 

| Solar-PuTTY *free tool*

Practical no.5

Implement Inter-VLAN Routing

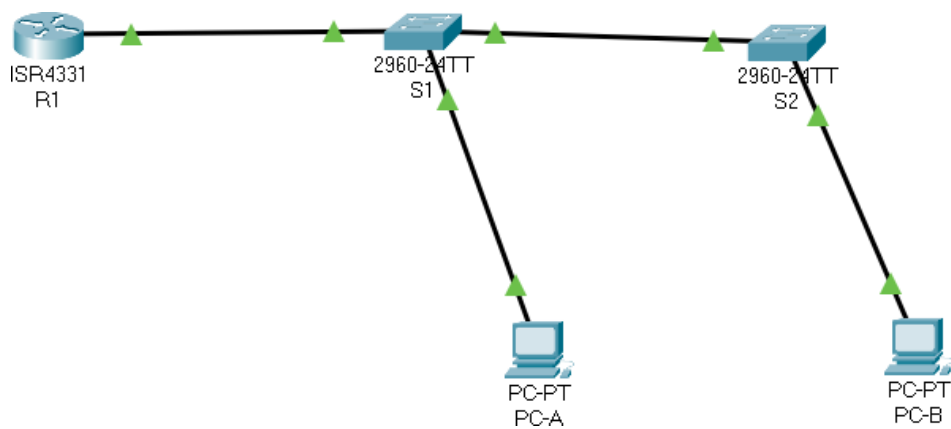
Aim: To implement Inter-VLAN Routing using Cisco Packet Tracer.

Requirement: Cisco Packet Tracer tool.


Procedure:

Part 1:

Step1: Build the Network and Configure Basic Device Settings:



Output:

 R1

Physical Config CLI Attributes

```
would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#Enable secret class
R1(config)#Line console 0 password
      ^
% Invalid input detected at '^' marker.

R1(config)#Line console 0
R1(config-line)#password cisco
R1(config-line)#Login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#Login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd $ Unauthorised access is prohibited $
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
R1#clock set 11:38:50 23 December 2021
```


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
5. Assign class as the privileged EXEC encrypted password.
R1(config)# enable secret class
6. Assign cisco as the console password and enable login.
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
7. Assign cisco as the vty password and enable login.
R1(config)# line vty 0 15
R1(config-line)# password cisco
R1(config-line)# login
8. Encrypt the plaintext passwords.
R1(config)# service password-encryption
9. 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
```

3. Assign class as the privileged EXEC encrypted password.

```
S1(config)# enable secret class
```

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

```
S1(config)# line console 0
```

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

```
S1(config-line)# login
```

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

```
S1(config)# line vty 0 15
```

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

```
S1(config-line)# login
```

6. Encrypt the plaintext passwords.

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

7. 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
```

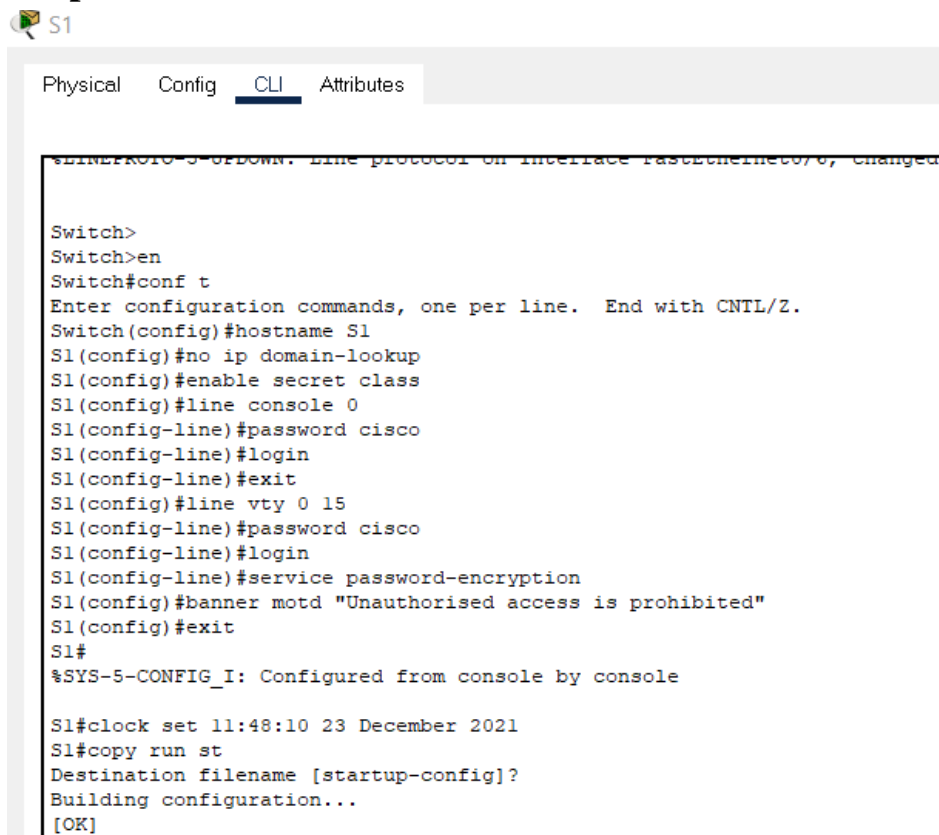
8. Set the clock on the switch.

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

9. Save the running configuration to the startup configuration.

```
S1# copy run st
```

Output:



The image shows a screenshot of the Cisco Packet Tracer interface. At the top, there are tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is selected. The main window displays the command-line interface for a switch named S1. The prompt is 'Switch>'. The user has entered 'en' to enter global configuration mode, resulting in 'Switch(config)#'. Then, 'conf t' is entered to enter configuration mode, resulting in 'Switch(config)#'. The user then enters a series of commands to configure the switch: 'hostname S1', 'no ip domain-lookup', 'enable secret class', 'line console 0', 'password cisco', 'login', 'exit', 'line vty 0 15', 'password cisco', 'login', 'service password-encryption', 'banner motd "Unauthorised access is prohibited"', and 'exit'. The prompt returns to 'Switch(config)#'. The user then enters 'clock set 11:48:10 23 December 2021', 'copy run st', and 'Building configuration...' followed by '[OK]'. The output shows the configuration commands being entered and the resulting prompts.

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd "Unauthorised access is prohibited"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#clock set 11:48:10 23 December 2021
S1#copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configure basic settings for Switch 2:

2. Assign a device name to the switch.
switch(config)# hostname S2
3. 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
4. Assign class as the privileged EXEC encrypted password.
S2(config)# enable secret class
5. Assign cisco as the console password and enable login.
S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login
6. Assign cisco as the vty password and enable login.
S2(config)# line vty 0 15

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

```
S2(config-line)# login
```

7. Encrypt the plaintext passwords.

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

8. 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
```

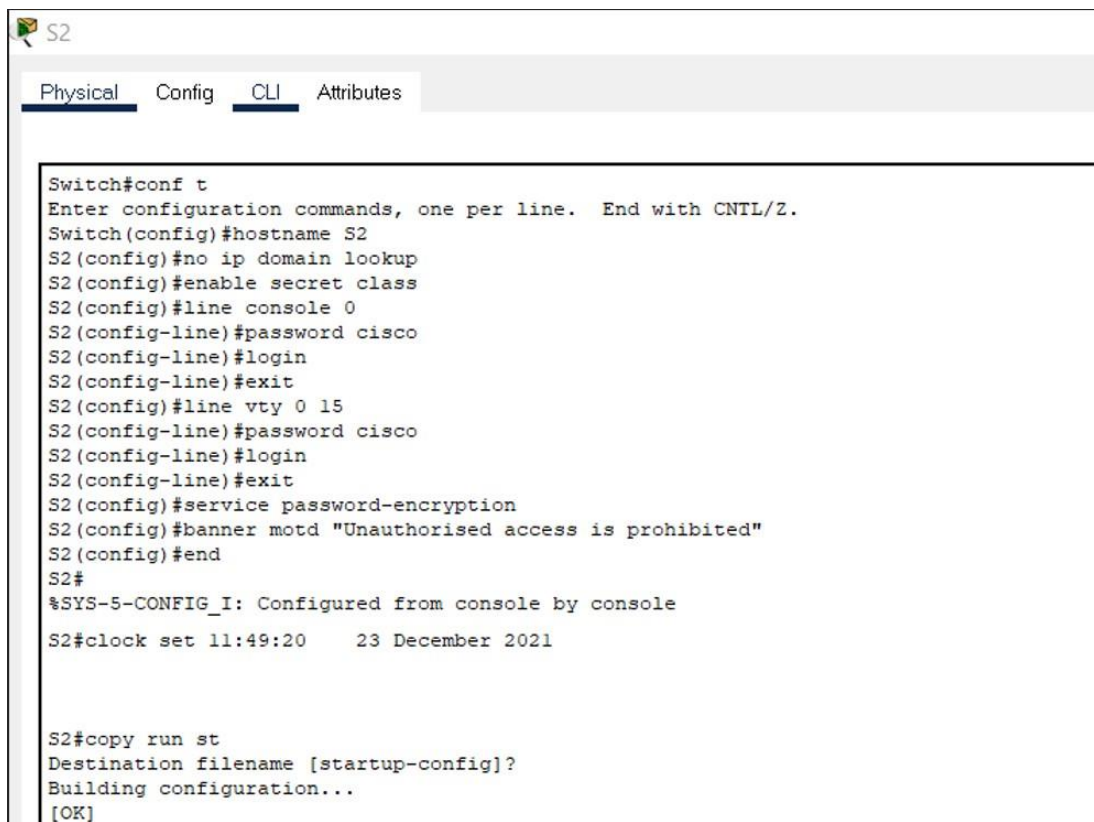
9. Set the clock on the switch.

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

10. Save the running configuration to the startup configuration.

```
S2# copy run st
```

Output:

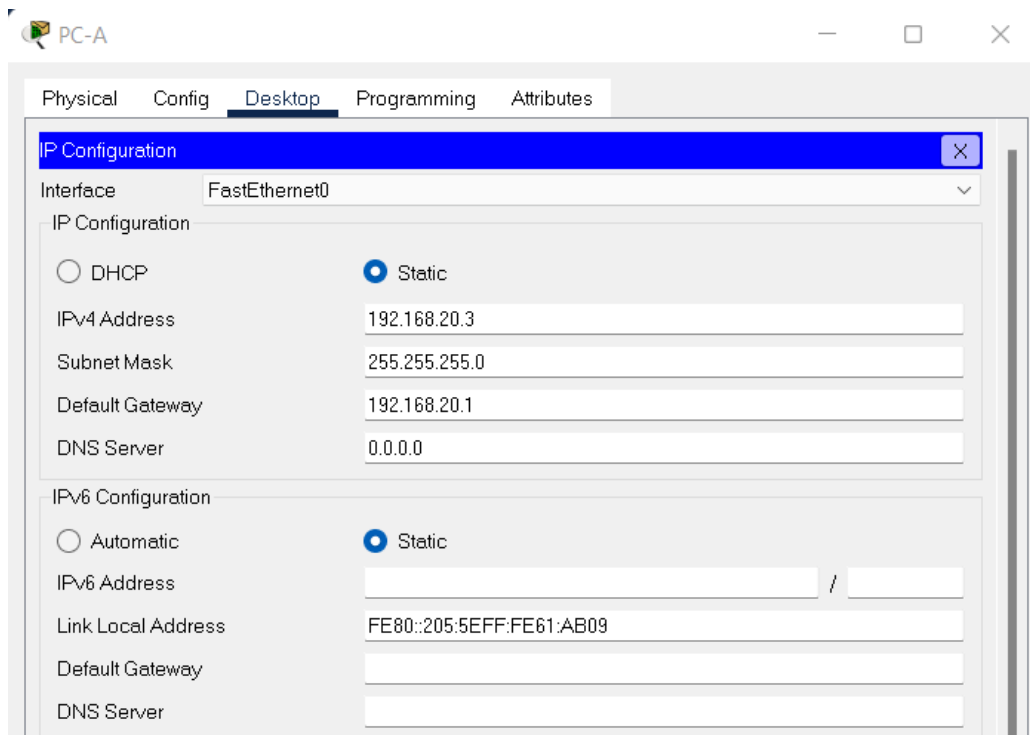


```
S2
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain lookup
S2(config)#enable secret class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd "Unauthorised access is prohibited"
S2(config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#clock set 11:49:20 23 December 2021

S2#copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
```

Step 4: Configure PC hosts.

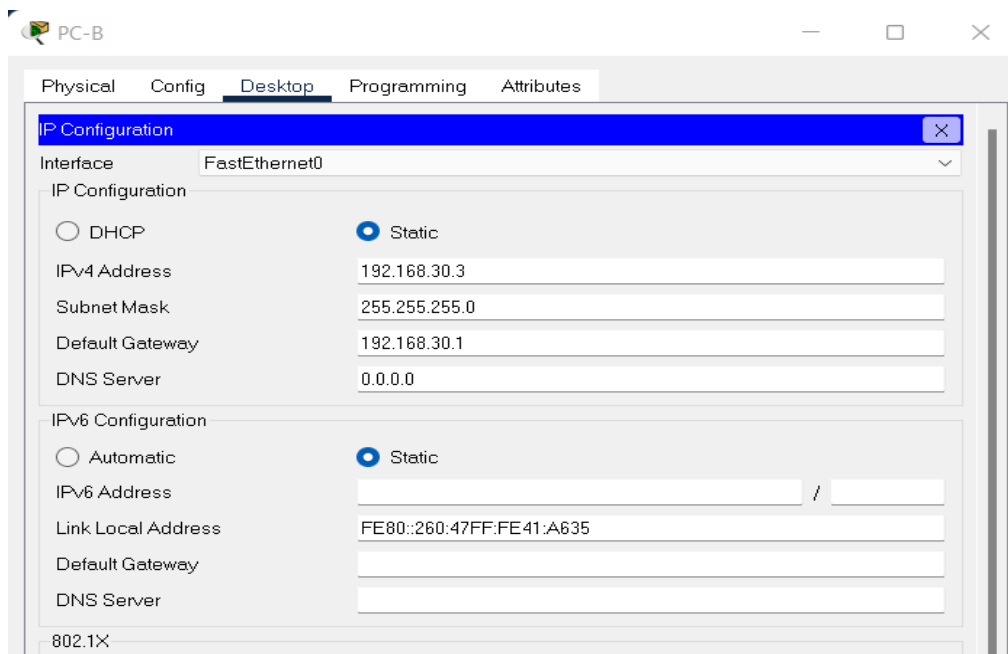
PC-A:



The screenshot shows the configuration window for PC-A. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected for both IPv4 and IPv6 configurations. The IPv4 configuration includes an address of 192.168.20.3, a subnet mask of 255.255.255.0, a default gateway of 192.168.20.1, and a DNS server of 0.0.0.0. The IPv6 configuration includes a static address, a link local address of FE80::205:5EFF:FE61:AB09, and empty fields for default gateway and DNS server.

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IPv4 Address	192.168.20.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::205:5EFF:FE61:AB09
Default Gateway	
DNS Server	

PC-B:



The screenshot shows the configuration window for PC-B. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected for both IPv4 and IPv6 configurations. The IPv4 configuration includes an address of 192.168.30.3, a subnet mask of 255.255.255.0, a default gateway of 192.168.30.1, and a DNS server of 0.0.0.0. The IPv6 configuration includes a static address, a link local address of FE80::260:47FF:FE41:A635, and empty fields for default gateway and DNS server.

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IPv4 Address	192.168.30.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.30.1
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::260:47FF:FE41:A635
Default Gateway	
DNS Server	

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
```

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#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
```

```

S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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

```

2. 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

```

```

S1(config)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

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

```

```

S2(config)#interface vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

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

```

3. 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
```

```
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

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

```
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
```

```
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

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

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
```



Physical Config CLI Attributes

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#exit
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#end
```



```

S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 30

```

```

S2(config-if-range)#exit
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#end
S2#

```

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

S1# show vlan brief

```

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, Gig0/1, Gig0/2
1000	Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```

S1#

```

S2# show vlan brief

```

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, Gig0/1, Gig0/2
1000	Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

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
```

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

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

3. 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
```

4. 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

```

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# int f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#switchport mode trunk
S1(config-if)#
S1(config-if)#switchport trunk native vlan 1000
S1(config-if)#switchport trunk allowed vlan 10,20,30,1000
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show interface 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:

2. Configure static trunking on interface F0/1 for both switches.
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
3. Set the native VLAN to 1000 on both switches.
S2(config-if)# switchport trunk native vlan 1000
4. 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
5. 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

```
S2#
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to uprt
% Incomplete command.
S2(config-if)#switchport mode trunk
S2(config-if)#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1000 on FastEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent local vlan.

S2(config-if)#switchport
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S1 FastEthernet0/1 (1000).

% Incomplete command.
S2(config-if)#switchport trunk native vlan 1000
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN1000. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port consistency restored.

S2(config-if)#switchport trunk allowed vlan 10,20,30,1000
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show interface 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:

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1000
S1(config-if)#exit
S1(config)#end
S1#
```

Switch 2:

```
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/5
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 1000
S2(config-if)#exit
S2(config)#end
S2#
```

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

S1# copy run st

```
S1#copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
```

S2# copy run st

```
S2#copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

3. 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.

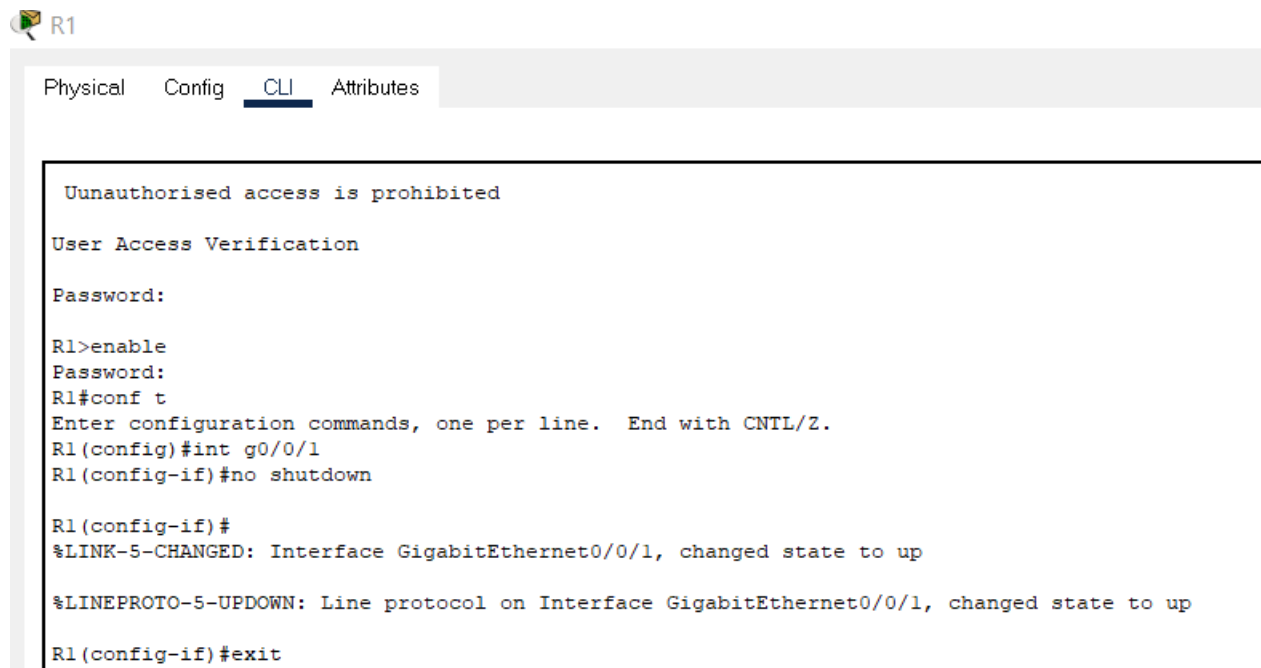
Part 4: Configure Inter-VLAN Routing on the Router

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
```



```
R1
Physical Config CLI Attributes

Unauthorised access is prohibited
User Access Verification
Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0/1
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
R1(config-if)#exit
```

2. 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:

```
R1(config)#int g0/0/1.10
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.10, changed state to up

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)#int g0/0/1.20
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.20, changed state to up

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)#int g0/0/1.20
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.20, changed state to up

R1(config-subif)#description Sales Network
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#int g0/0/1.30
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.30, changed state to up

R1(config-subif)#description Operations Network
R1(config-subif)#ip address 192.168.30.1 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#int g0/0/1.1000
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.1000, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.1000, changed state to up

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

3). Verify the sub-interfaces are operational

R1# show ip interface brief

```
R1#show ip interface brief
Interface          IP-Address      OK? Method Status              Protocol
GigabitEthernet0/0/0  unassigned     YES unset  administratively down down
GigabitEthernet0/0/1  unassigned     YES unset  up                  up
GigabitEthernet0/0/1.10 192.168.10.1   YES manual up                  up
GigabitEthernet0/0/1.20 192.168.20.1   YES manual up                  up
GigabitEthernet0/0/1.30 192.168.30.1   YES manual up                  up
GigabitEthernet0/0/1.100 unassigned     YES unset  up                  up
GigabitEthernet0/0/2  unassigned     YES unset  administratively down down
Vlan1               unassigned     YES unset  administratively down down
R1#
```

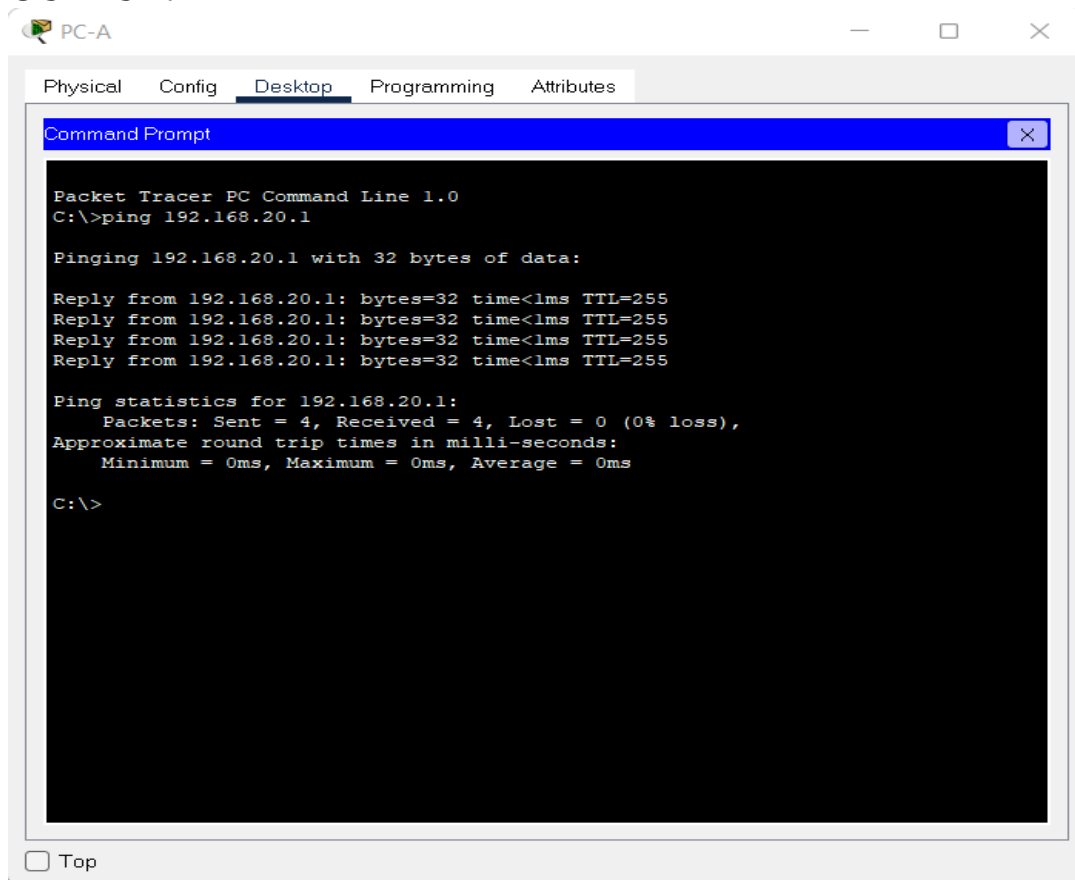
Part 5: Verify Inter-VLAN Routing is Working

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:-



2. Ping from PC-A to PC-B

Output:

```
C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.3: bytes=32 time=1ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127
Reply from 192.168.30.3: bytes=32 time=13ms TTL=127
Reply from 192.168.30.3: bytes=32 time<1ms TTL=127

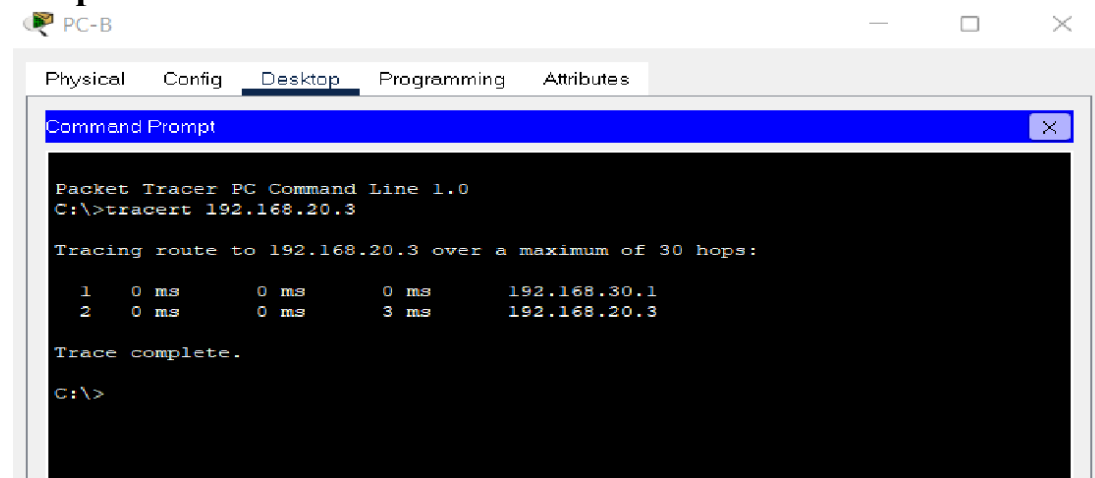
Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

3. 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:



The screenshot shows a Packet Tracer PC window for PC-B. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The Command Prompt shows the execution of the 'tracert 192.168.20.3' command. The output indicates a successful trace to 192.168.20.3 over 2 hops. The first hop is 192.168.30.1 with 0 ms delay, and the second hop is 192.168.20.3 with 3 ms delay. The trace is complete.

```
Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.20.3

Tracing route to 192.168.20.3 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.30.1
  2  0 ms    0 ms    3 ms    192.168.20.3

Trace complete.

C:\>
```

