NST21022 - Practical for Network Switching and Routing

Department of Information and Communication Technology

Faculty of Technology

Lab sheet :16
Reg. Number: SEU/IS/20/ICT/084
Academic Year :2020/2021
Practical No :16

Title: Configure EtherChannel, HSRP and Switch Security

Aim:

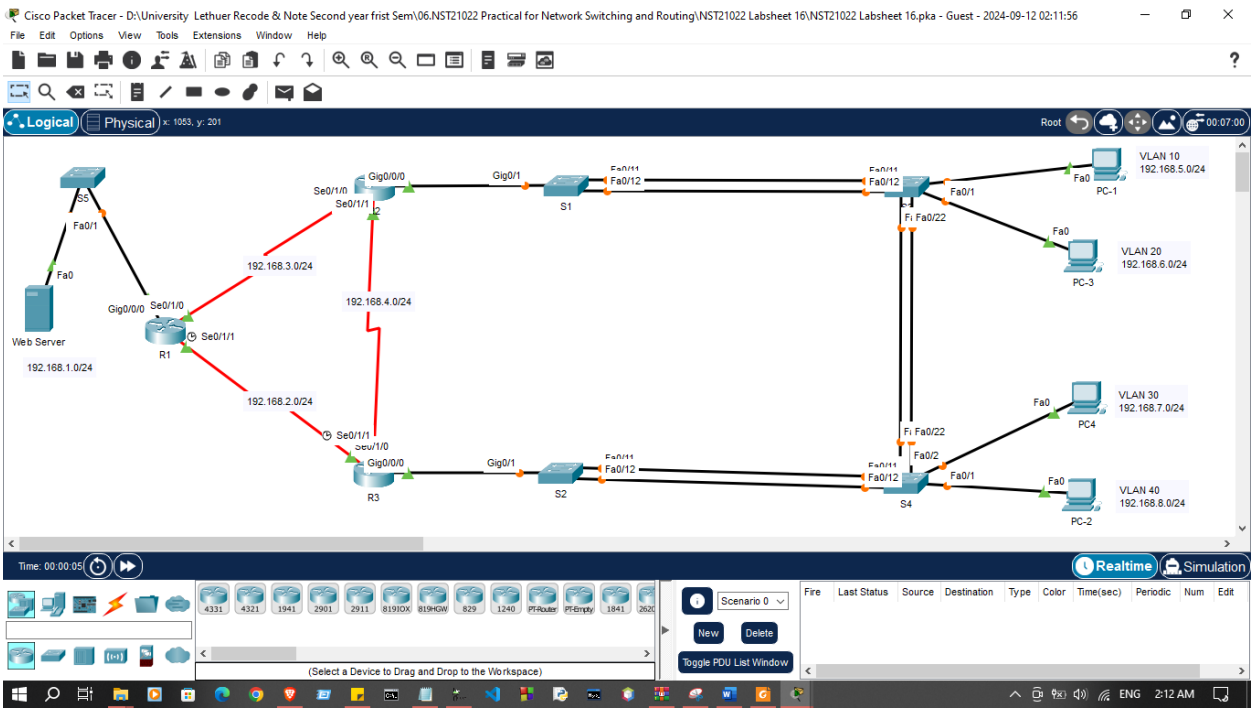
- Configure EtherChannel
- Configure HSRP (Hot Standby Router Protocol)
- Configure Switch Security

Task:

- Configure an EtherChannel with Cisco Pag
- Configure an 802.3ad LACP EtherChannel
- Configure a Redundant EtherChannel Link
- Configure an HSRP active router
- Configure an HSRP standby router
- Secure Trunk
- Secure Unused Switchports
- Implement Port Security
- Enable DHCP Snooping
- Configure Rapid PVST Port Fast and BPDU Guard

Activities

Use "NST21022 Lab sheet 16.pka" file



Addressing Table

Device	Interface	IP Address	Default Gateway
R1	G0/0/0	192.168.1.1	N/A
	S0/1/0	192.168.3.1	
	S0/1/1	192.168.2.1	
R2	G0/0/0.10	192.168.5.1	N/A
	G0/0/0.20	192.168.6.1	
	S0/1/0	192.168.3.2	
	S0/1/1	192.168.4.1	
R3	G0/0/0.30	192.168.7.1	N/A
	G0/0/0.40	192.168.8.1	
	S0/1/0	192.168.2.2	
	S0/1/1	192.168.4.2	
HSRP Virtual Gateway	Virtual	192.168.6.254	
Web Server	NIC	192.168.1.10	192.168.1.1
PC-1	NIC	192.168.5.10	192.168.5.1
PC-2	NIC	192.168.8.10	192.168.8.1
PC-3	NIC	192.168.6.10	192.168.6.1
PC-4	NIC	192.168.7.10	192.168.7.1

Exercise 01: Configure EtherChannel

Channel Group	Ports	Protocol
1	S1 F0/11, F0/12 S3 F0/11, F0/12	PAgP
2	S2 F0/11, F0/12 S4 F0/11, F0/12	LACP
3	S3 F0/21, F0/22 S4 F0/21, F0/22	Negotiated LACP

1. Configure an EtherChannel with Cisco PAgP on S1 and S3

```
S1(config)# interface range f0/11– 12
S1(config-if-range)# shutdown
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown

S3(config)# interface range f0/11-12
S3(config-if-range)# shutdown
S3(config-if-range)# channel-group 1 mode desirable
S3(config-if-range)# no shutdown
```

S1>enable
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)#interface range fa0/11-12
S1(config-if-range)#shutdown

S1(config-if-range)#channel-group 1 mode desirable
S1(config-if-range)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to down

Creating a port-channel interface Port-channel 1

```
S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#interface range fa0/11-12
S1(config-if-range)#shutdown


S1(config-if-range)#channel-group 1 mode desirable
S1(config-if-range)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to down

Creating a port-channel interface Port-channel 1
```

S3>enable
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#
S3(config)#interface range fa0/11-12

S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
S3(config-if-range)#channel-group 1 mode desirable
S3(config-if-range)#no shutdown
Creating a port-channel interface Port-channel 1

```
S3>enable
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#
S3(config)#interface range fa0/11-12
S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
S3(config-if-range)#channel-group 1 mode desirable
S3(config-if-range)#no shutdown
Creating a port-channel interface Port-channel 1
```

2. Configure the logical interface to become a trunk by first entering the interface port-channel number command and then the switchport mode trunk command

S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk

S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk

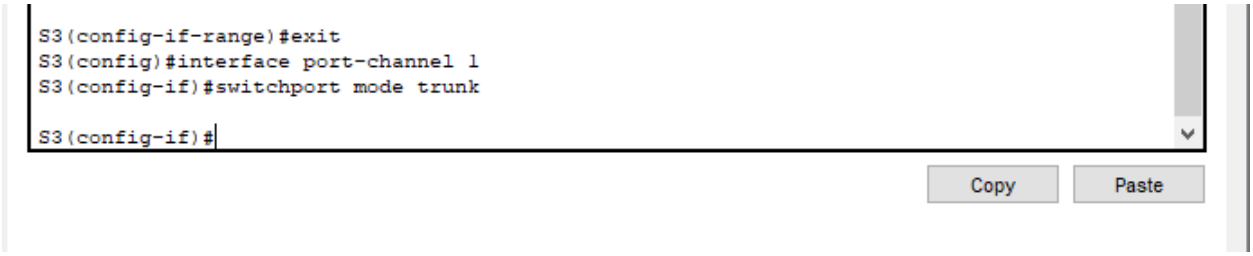
S1(config-if-range)#
S1(config-if-range)#exit
S1(config)#interface port-channel 1
S1(config-if)#switchport mode trunk

S1(config-if)#

```
S1(config-if-range)#
S1(config-if-range)#exit
S1(config)#interface port-channel 1
S1(config-if)#switchport mode trunk

S1(config-if)#
```

Copy Paste

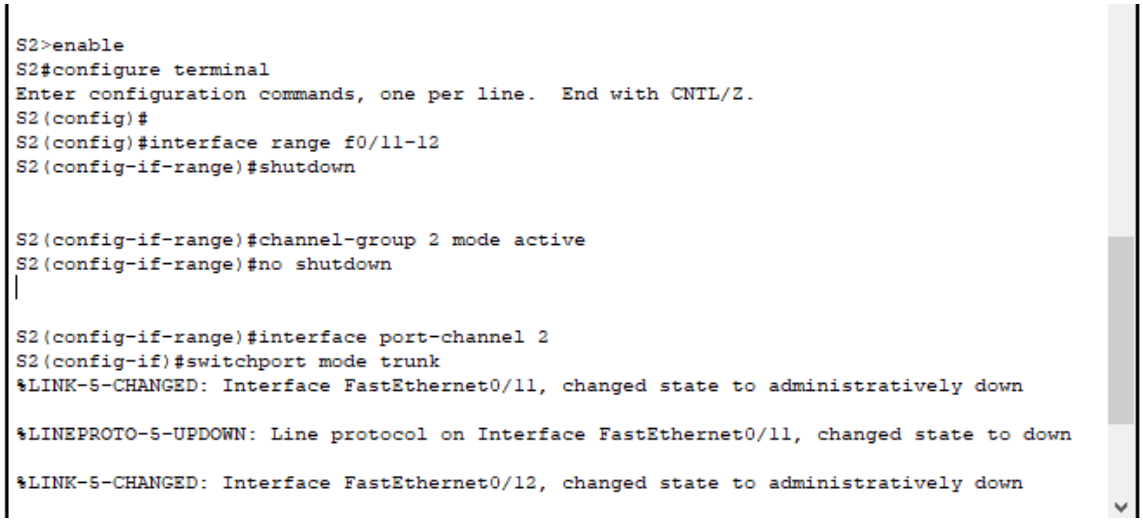
S3(config-if-range)#exit
S3(config)#interface port-channel 1
S3(config-if)#switchport mode trunk
S3(config-if)#



3. Configure an 802.3ad LACP EtherChannel on S2 and S4

S2(config)# interface range f0/11 - 12
S2(config-if-range)# shutdown
S2 (config-if-range)# channel-group 2 mode active
S2(config-if-range)# no shutdown
S2(config-if-range)# interface port-channel 2
S2(config-if)# switchport mode trunk

S2>enable
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#
S2(config)#interface range f0/11-12
S2(config-if-range)#shutdown
S2(config-if-range)#channel-group 2 mode active
S2(config-if-range)#no shutdown
S2(config-if-range)#interface port-channel 2
S2(config-if)#switchport mode trunk



4. Configure a Redundant EtherChannel Link on S3

S3(config)# interface range f0/21 - 22
S3(config-if-range)# shutdown
S3(config-if-range)# channel-group 3 mode passive
S3(config-if-range)# no shutdown
S3(config-if-range)# interface port-channel 3
S3(config-if)# switchport mode trunk

S3(config)#interface range f0/21 - 22
S3(config-if-range)#shutdown
S3(config-if-range)#channel-group 3 mode passive
S3(config-if-range)#no shutdown
S3(config-if-range)#interface port-channel 3
S3(config-if)#switchport mode trunk

```
S3(config)#interface range f0/21 - 22
S3(config-if-range)#shutdown


S3(config-if-range)#channel-group 3 mode passive
S3(config-if-range)#no shutdown


S3(config-if-range)#interface port-channel 3
S3(config-if)#switchport mode trunk
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down
```

5. On S4, add ports F0/21 and F0/22 to Port Channel 3 with the channel-group 3 mode active command.

S4>enable
S4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S4(config)#
S4(config)#interface range f0/21-22
S4(config-if-range)#channel-group 3 mode active
S4(config-if-range)#no shutdown
S4(config-if-range)#interface port-channel 3
S4(config-if)#switchport mode trunk
Creating a port-channel interface Port-channel 3

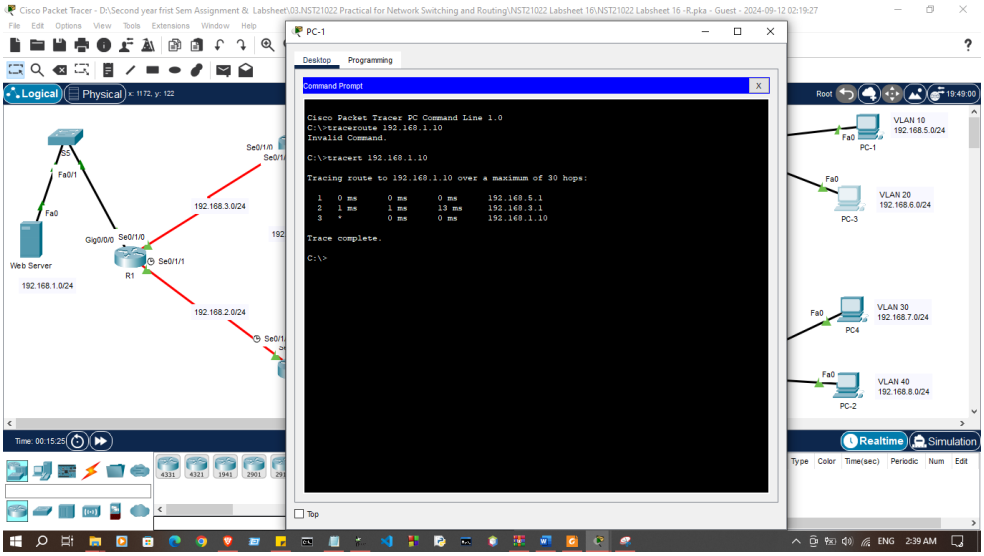
```
S4>enable
S4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S4(config)#
S4(config)#interface range f0/21-22
S4(config-if-range)#channel-group 3 mode active
S4(config-if-range)#no shutdown
S4(config-if-range)#interface port-channel 3
S4(config-if)#switchport mode trunk
Creating a port-channel interface Port-channel 3
```

S4(config-if)#interface range f0/11-12
S4(config-if-range)#shutdown
S4(config-if-range)#channel-group 2 mode active
S4(config-if-range)#no shutdown
S4(config-if-range)#interface port-channel 2
S4(config-if)#switchport mode trunk

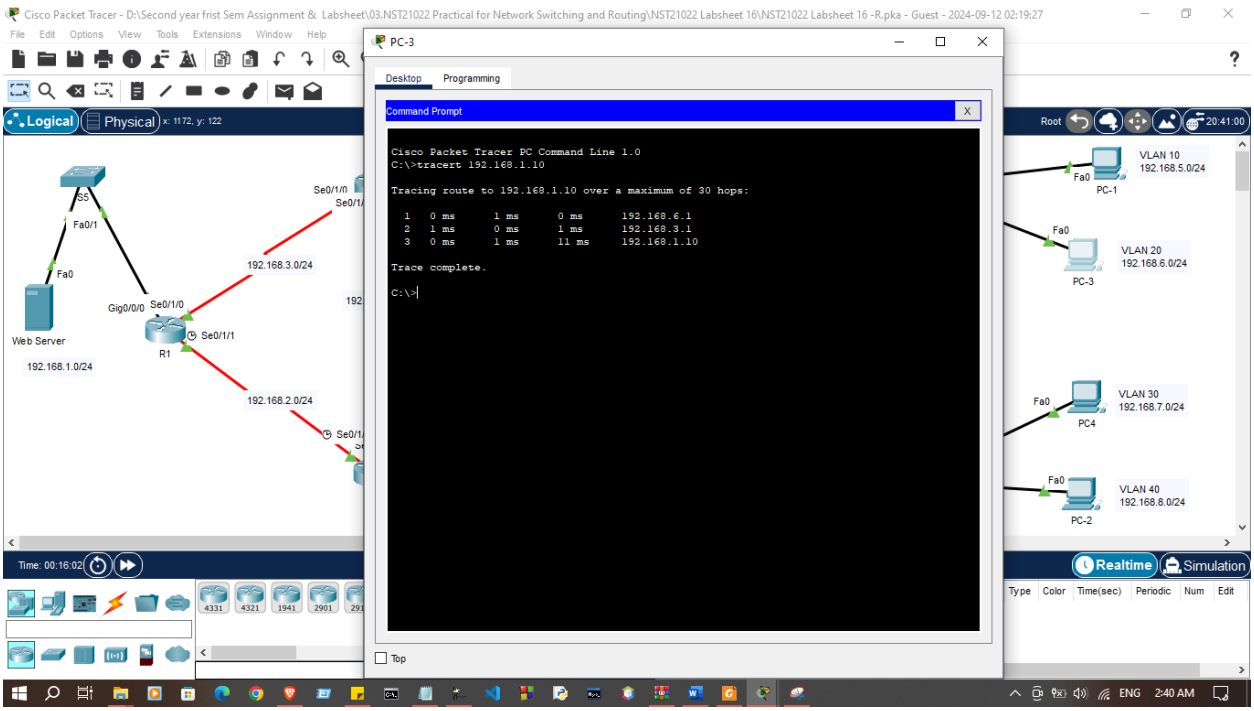
```
S4(config-if)#interface range f0/11-12
S4(config-if-range)#shutdown


S4(config-if-range)#channel-group 2 mode active
S4(config-if-range)#no shutdown


S4(config-if-range)#interface port-channel 2
S4(config-if)#switchport mode trunk
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
```

Exercise 02: Configure HSRP (Hot Standby Router Protocol)

1. Trace the path to the Web Server from PC-1



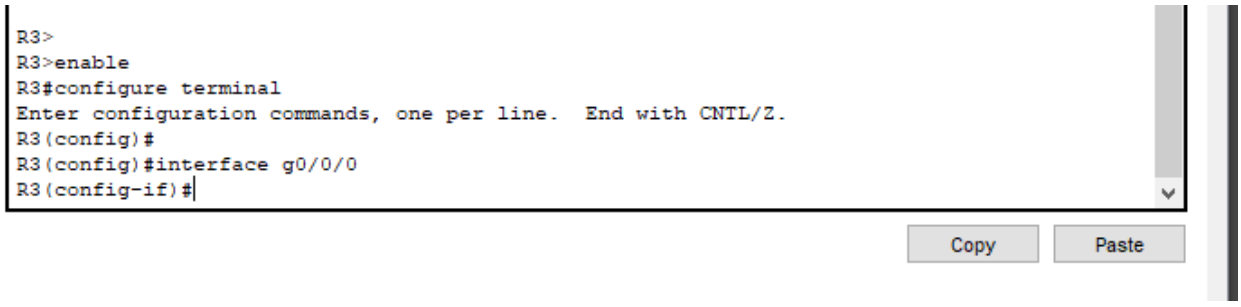
2. Trace the path to the Web Server from PC-3



3. Configure HSRP on R3

R3(config)# interface g0/0/0

R3>
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#interface g0/0/0
R3(config-if)#



4. Specify the HSRP protocol version number. The most recent version is version Note: Standby version 1 only supports IPv4 addressing

R3(config-if)# standby version 2

R3(config)#interface g0/0/0
R3(config-if)#standby version 2
R3(config-if)#

```
R3(config)#
R3(config)#interface g0/0/0
R3(config-if)#standby version 2
R3(config-if)#
```

Copy Paste

5. Configure the IP address of the virtual default gateway

R3(config-if)# standby 1 ip 192.168.6.254

R3(config-if)#standby version 2
R3(config-if)#standby 1 ip 192.168.6.254
% Warning: address is not within a subnet on this interface
R3(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0 Grp 1 state Init -> Init

```
R3(config)#interface g0/0/0
R3(config-if)#standby version 2
R3(config-if)#standby 1 ip 192.168.6.254
% Warning: address is not within a subnet on this interface
R3(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0 Grp 1 state Init -> Init

R3(config-if)#
```

6. Designate the active router for the HSRP group

R3(config-if)# standby 1 priority 150

R3(config-if)#standby 1 priority 150
R3(config-if)#

```
R3(config-if)#standby 1 priority 150
R3(config-if)#
R3#
```

7. R3 will operate as the active router and traffic from the two LANs will use it as the default gateway

R1(config-if)# standby 1 preempt

R3(config-if)#standby 1 priority 150
R3(config-if)#standby 1 preempt
R3(config-if)#

```
R3(config-if)#standby 1 priority 150
R3(config-if)#standby 1 preempt
R3(config-if)#
```

Copy Paste

8. Repeat step 4, 5 on R2 G0/0/0 interface to make standby router

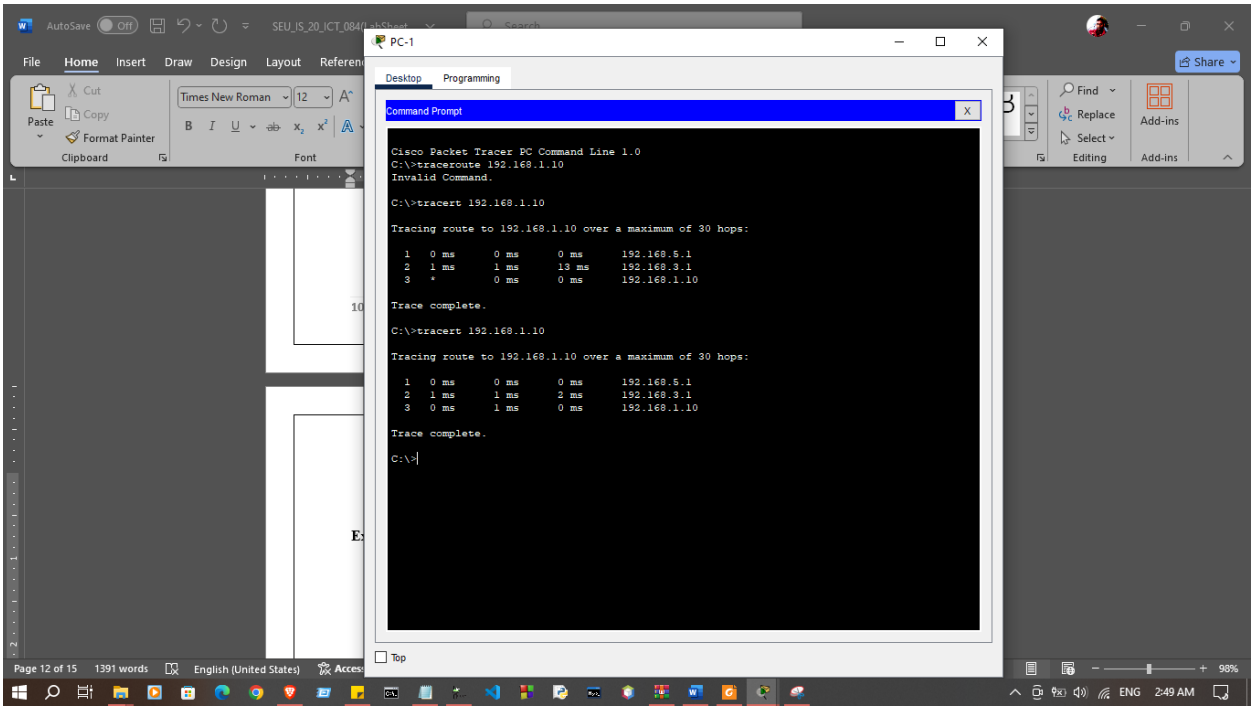
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface g0/0/0
R2(config-if)#standby version 2
R2(config-if)#standby 1 ip 192.168.6.254
% Warning: address is not within a subnet on this interface
R2(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0 Grp 1 state Init -> Init

R2(config-if)#

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface g0/0/0
R2(config-if)#standby version 2
R2(config-if)#standby 1 ip 192.168.6.254
% Warning: address is not within a subnet on this interface
R2(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0 Grp 1 state Init -> Init

R2(config-if)#
```

Copy Paste

9. Verify HSRP configuration using ***tracert*** command



Exercise 03: Configure Switch Security

Switch	VLAN Number	VLAN Name	Port Member	Network
S1	**100**	**Native**	**--**	**--**
S3	**10**	**Sales**	**F0/1**	**192.168.5.0/24**
	20	**Production**	**F0/2**	**192.168.6.0/24**
	999	**BlackHole**	**Unused**	**--**
S4	**30**	**Accounts**	**F0/2**	**192.168.8.0/24**
	40	**Finance**	**F0/1**	**192.168.7.0/24**

1. Disable DTP negotiation on S1 G0/1 interface.

S1(config-if)#switchport nonegotiate

S1(config)#interface GigabitEthernet0/1
S1(config-if)#switchport trunk native vlan 100
S1(config-if)#switchport nonegotiate

S1(config-if)#

```
S1>en
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface GigabitEthernet0/1
S1(config-if)#switchport trunk native vlan 100
S1(config-if)#switchport nonegotiate
S1(config-if)#
```

Copy Paste

.

2. Create VLAN 100 and give it the name Native on S1 and Configure G0/1 trunk port use VLAN 100 as the native VLAN.

S1(config)#vlan 100
S1(config-vlan)#name Native
S1(config)#interface GigabitEthernet0/1
S1(config-if)#switchport trunk native vlan 100

S1(config)#vlan 100
S1(config-vlan)#name Native
S1(config-vlan)#interface GigabitEthernet0/1
S1(config-if)#switchport trunk native vlan 100
S1(config-if)#

3. Secure Unused Switchport
    a. Shutdown all unused switch ports on S3.

S3(config)#interface range F0/3-10, F0/13-20, F0/23-24, G0/1-2
S3(config-if-range)#shutdown
S3(config-if-range)#exit

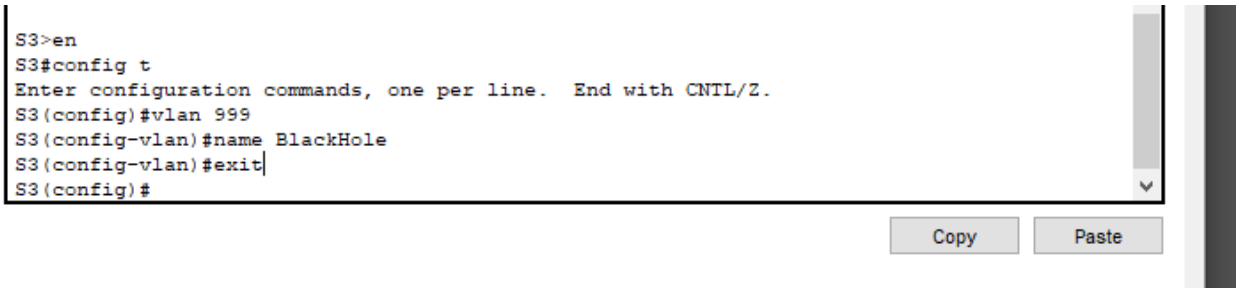
```
S1(config)#vlan 100
S1(config-vlan)#name Native
S1(config-vlan)#interface GigabitEthernet0/1
S1(config-if)#switchport trunk native vlan 100
S1(config-if)#
```

Copy Paste

    b. On S3, create a VLAN 999 and name it BlackHole. The configured name must match the requirement exactly.

S3(config)#vlan 999
S3(config-vlan)#name BlackHole
S3(config-vlan)#exit

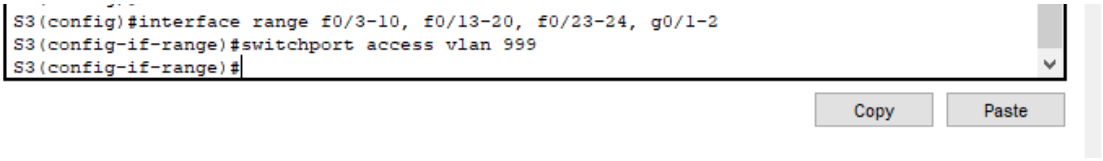
S3>en
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 999
S3(config-vlan)#name BlackHole
S3(config-vlan)#exit
S3(config)#



c. Move all unused switch ports to the BlackHole VLAN.

S3(config)#interface range F0/3-10, F0/13-20, F0/23-24, G0/1-2
S3(config-if-range)#switchport access vlan 999

S3(config)#interface range f0/3-10, f0/13-20, f0/23-24, g0/1-2
S3(config-if-range)#switchport access vlan 999
S3(config-if-range)#



4. Implement Port Security
   a. Activate port security on all the active access ports on switch S3

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport port-security

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport port-security
S3(config-if-range)#
S3(config-if-range)#

```
S3(config)#
S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport port-security
S3(config-if-range)#
S3(config-if-range)#
```

Copy Paste

b. Configure the active ports to allow a maximum of 4 MAC addresses to be learned on the ports.

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport port-security maximum 4

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport port-security maximum 4
S3(config-if-range)#

```
S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport port-security maximum 4
S3(config-if-range)#
```

Copy Paste

c. For ports F0/1 on S3, statically configure the MAC address of the PC using port security.

S3(config)#interface FastEthernet0/1
S3(config-if)#switchport port-security mac-address <<PC-Add>>

S3(config-if)#interface FastEthernet0/1
S3(config-if)#switchport port-security mac-address 000D.BD05.152D
Found duplicate mac-address 000d.bd05.152d.
S3(config-if)#
S3(config-if)#

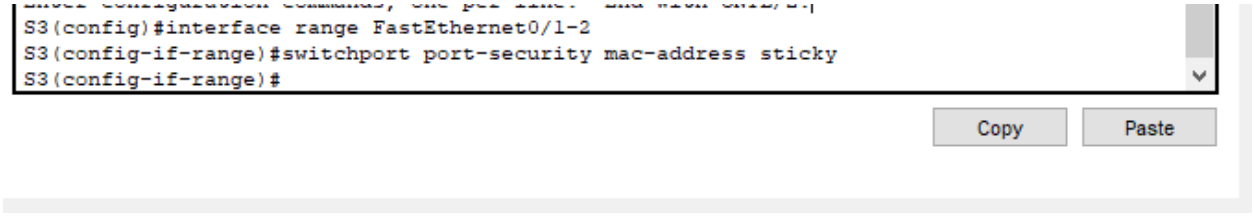
```
S3(config-if)#
S3(config-if)#interface FastEthernet0/1
S3(config-if)#switchport port-security mac-address 000D.BD05.152D
Found duplicate mac-address 000d.bd05.152d.
S3(config-if)#
S3(config-if)#
```

Copy Paste

d. Configure each active access port so that it will automatically add the MAC addresses learned on the port to the running configuration.

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport port-security mac-address sticky

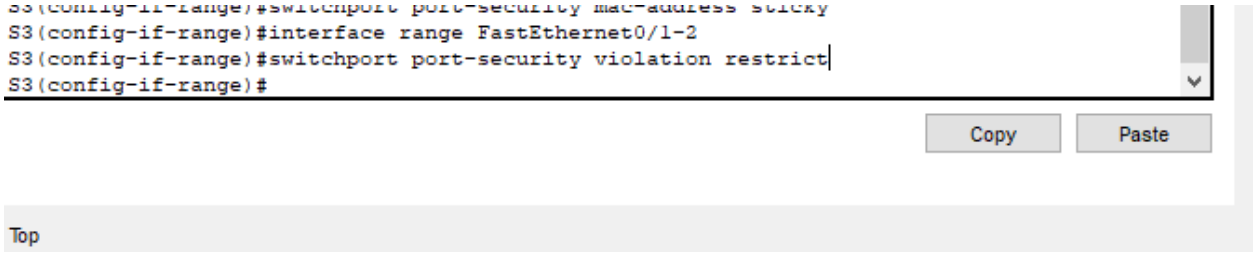
S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport port-security mac-address sticky
S3(config-if-range)#



e. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum, generate a Syslog entry, but not disable the ports.

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport port-security violation restrict

S3(config-if-range)#interface range FastEthernet0/1-2
S3(config-if-range)#switchport port-security violation restrict
S3(config-if-range)#



5. Configure DHCP Snooping
   a. Configure the trunk ports on S3 as trusted ports.

S3(config)#interface range FastEthernet0/11-12
S3(config-if-range)#ip dhcp snooping trust

S3(config)#interface range FastEthernet0/11-12
S3(config-if-range)#ip dhcp snooping trust
S3(config-if-range)#

```
S3(config)#interface range FastEthernet0/11-12
S3(config-if-range)#ip dhcp snooping trust
S3(config-if-range)#
```

Copy Paste

b. Limit the untrusted ports on S3 to five DHCP packets per second.

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#ip dhcp snooping limit rate 5

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#ip dhcp snooping limit rate 5
S3(config-if-range)#

```
S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#ip dhcp snooping limit rate 5
S3(config-if-range)#
```

Copy Paste

Top

c. On S4, enable DHCP snooping globally and for VLANs 30 and 40.

S4(config)#ip dhcp snooping
S4(config)#ip dhcp snooping vlan 30,40

S4(config)#ip dhcp snooping
S4(config)#ip dhcp snooping vlan 30,40
S4(config)#

```
S4(config)#
S4(config)#ip dhcp snooping
S4(config)#ip dhcp snooping vlan 30,40
S4(config)#
```

Copy Paste

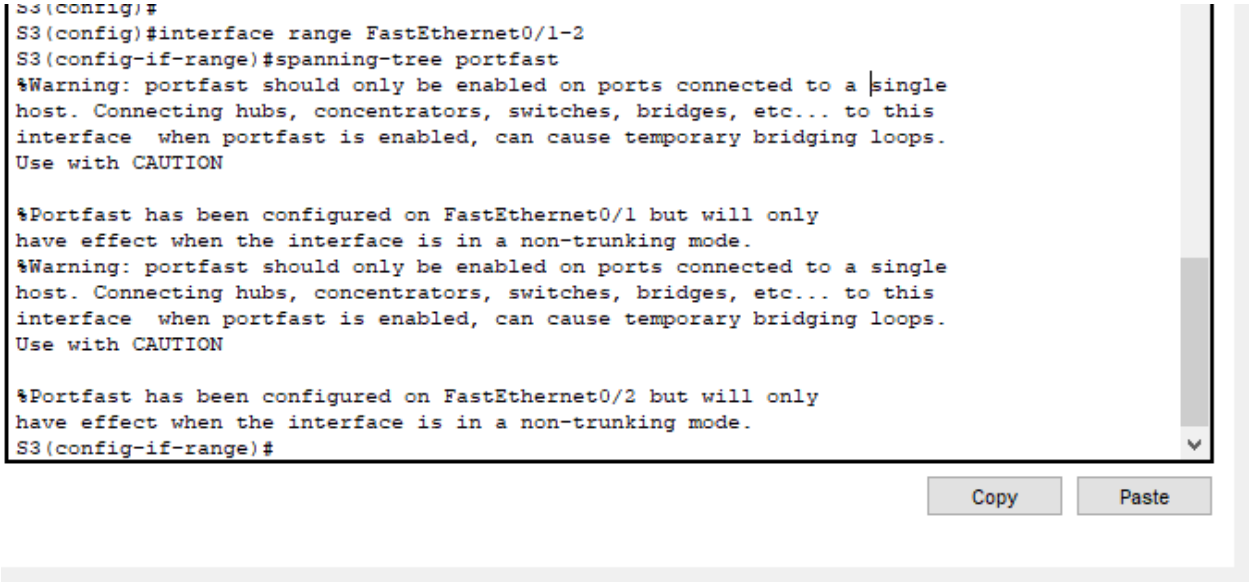
6. Configure PortFast, and BPDU Guard
   a. Enable PortFast on all the access ports that are in use on S3.

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#spanning-tree portfast

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only have effect when the interface is in a non-trunking mode.
S3(config-if-range)#



b. Enable BPDU Guard on all the access ports that are in use on S3.

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#spanning-tree bpduguard enable

S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#spanning-tree bpduguard enable
S3(config-if-range)#
S3(config-if-range)#

```
S3(config-if-range)#exit
S3(config)#
S3(config)#interface range FastEthernet0/1-2
S3(config-if-range)#spanning-tree bpduguard enable
S3(config-if-range)#
S3(config-if-range)#
```

Copy Paste

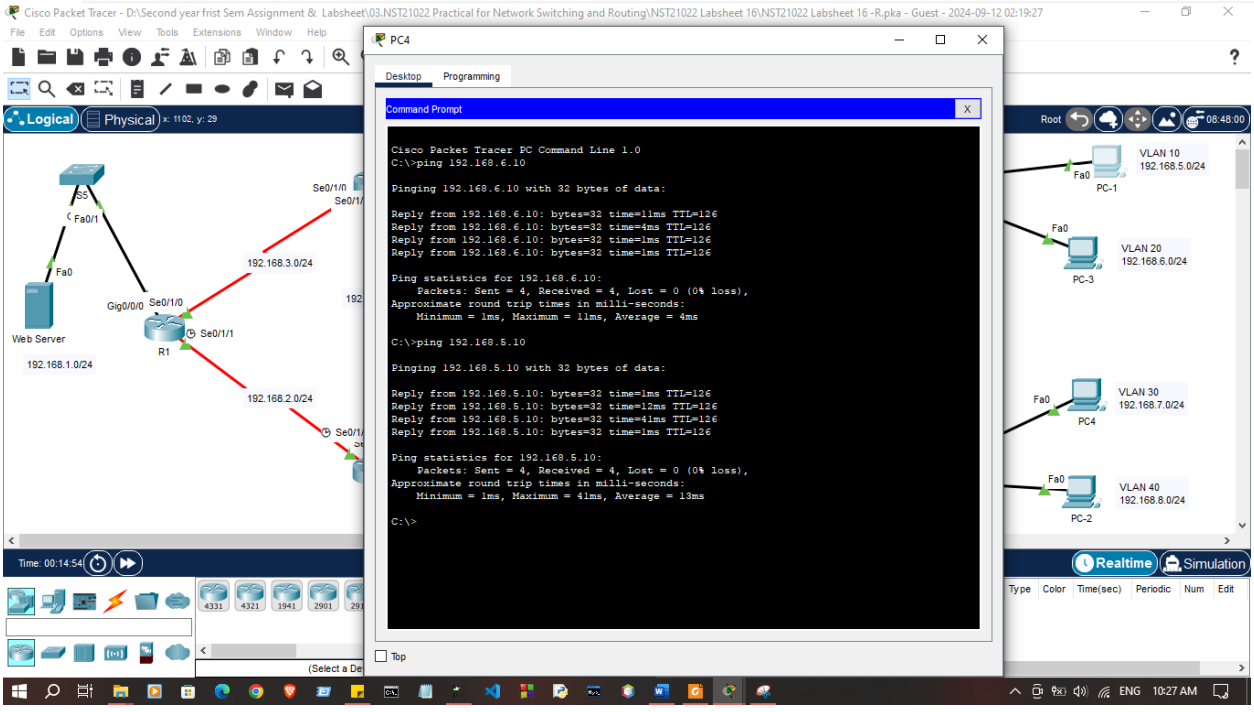
c. Configure S4 so that all access ports will use PortFast by default.

S4(config)#spanning-tree portfast default

S4(config)#spanning-tree portfast default
S4(config)#

```
S4(config)#ip dhcp snooping vlan 30,40
S4(config)#
S4(config)#spanning-tree portfast default
S4(config)#
```

Copy Paste



Discussion

- In this lab session, we explored advanced switch configurations including EtherChannel, HSRP, and switch security. We started by configuring an EtherChannel using Cisco's PAgP protocol and also set up an 802.3ad LACP EtherChannel for link aggregation to increase bandwidth and provide redundancy. To further ensure redundancy, we configured a backup EtherChannel link. Moving on to Hot Standby Router Protocol (HSRP), we set up both an active and a standby router to maintain network availability in case of failure. For security, we secured trunk links, disabled unused switch ports, implemented port security to control device access, and enabled DHCP snooping to prevent rogue DHCP servers. Additionally, we configured Rapid PVST PortFast to speed up port initialization and BPDU Guard to protect the network from potential loops. These tasks provided a comprehensive understanding of creating a secure and redundant switch environment.