Lab Sheet – 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 PAgP
- 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 PortFast and BPDU Guard

Activities

Use "NST21022 Labsheet 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
```

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
```

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
```

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
```

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

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
```

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
```

5. Configure the IP address of the virtual default gateway

```
R3(config-if)# standby 1 ip 192.168.6.254
```

6. Designate the active router for the HSRP group

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

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
```

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

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
```

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
```

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
```

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
```

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
```

   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
```

   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>>
```

   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
```

   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
```

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
```

   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
```

   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
```

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

    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

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

        S4(config)#spanning-tree portfast default