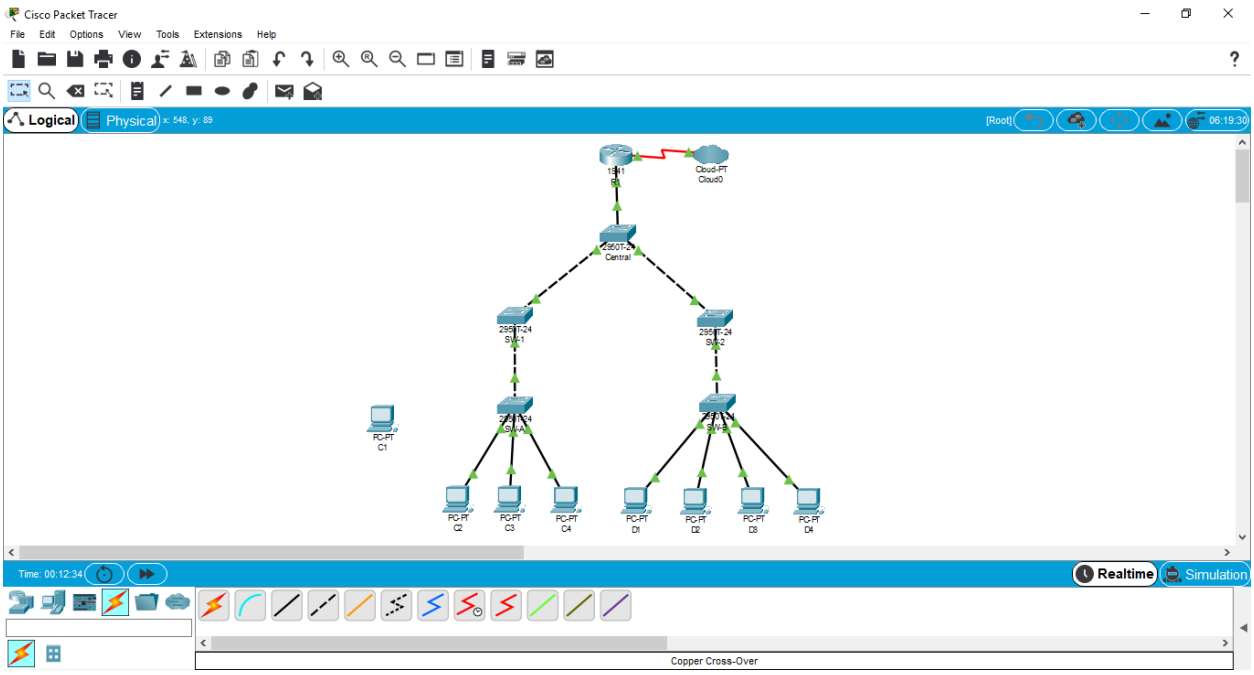
PRACTICAL 9

Aim : Layer 2 VLAN Security

a. Connect a new redundant link between SW-1 and SW-2.
b. Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
c. Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
d. Implement an ACL to prevent outside users from accessing the management VLAN.

Topology Diagram :



Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).

Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

Part 2: Create a Redundant Link Between SW-1 and SW-2

Step 1: Connect SW-1 and SW-2. Using a crossover cable, connect port F0/23 on SW-1 to port F0/23 on SW-2.

Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both SW-1 and SW-2, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.

```
SW-1(config)#interface f0/23
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#switchport trunk native vlan 15
SW-1(config-if)#switchport nonegotiate
SW-1(config-if)#no shutdown
```

```
SW-2(config)#interface f0/23
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#switchport trunk native vlan 15
SW-2(config-if)#switchport nonegotiate
SW-2(config-if)#no shutdown
```

Part 3: Enable VLAN 20 as a Management VLAN

The network administrator wants to access all switch and routing devices using a management PC. For security purposes, the administrator wants to ensure that all managed devices are on a separate VLAN.

Step 1: Enable a management VLAN (VLAN 20) on SW-A.

a. Enable VLAN 20 on SW-A

```
SW-A(config)#vlan 20
SW-A(config-vlan)#exit
```

b. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

```
SW-A(config)#interface vlan 20
SW-A(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SW-A(config-if)#ip address 192.168.20.1 255.255.255.0
```

Step 2: Enable the same management VLAN on all other switches.

a. Create the management VLAN on all switches: SW-B, SW-1, SW-2, and Central.

```
SW-B(config)#vlan 20
SW-B(config-vlan)#exit
```

```
SW-1(config)#vlan 20
SW-1(config-vlan)#exit
```

```
SW-2(config)#vlan 20
SW-2(config-vlan)#exit
```

```
Central(config)#vlan 20
Central(config-vlan)#exit
```

b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.

```
SW-B(config)#interface vlan 20
SW-B(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SW-B(config-if)#ip address 192.168.20.2 255.255.255.0
```

```
SW-1(config)#interface vlan 20
SW-1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SW-1(config-if)#ip address 192.168.20.3 255.255.255.0
```

```
SW-2(config)#interface vlan 20
SW-2(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
SW-2(config-if)#ip address 192.168.20.4 255.255.255.0
```

```
Central(config)#interface vlan 20
Central(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Central(config-if)#ip address 192.168.20.5 255.255.255.0
```

Step 3: Connect and configure the management PC.

Connect the management PC to SW-A port F0/1 and ensure that it is assigned an available IP address within the 192.168.20.0/24 network.

Step 4: On SW-A, ensure the management PC is part of VLAN 20.

Interface F0/1 must be part of VLAN 20.

```
SW-A(config-if)#interface f0/1
SW-A(config-if)#switchport access vlan 20
SW-A(config-if)#no shutdown
```

Step 5: Verify connectivity of the management PC to all switches.

The management PC should be able to ping SW-A, SW-B, SW-1, SW-2, and Central.

Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

a. Create subinterface g0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20

```
R1(config)# interface g0/0.3
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.3, changed state to up

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

b. Assign an IP address within the 192.168.20.0/24 network.

```
R1(config-subif)#interface g0/0.3
R1(config-subif)#ip address 192.168.20.100 255.255.255.0
```

Step 2: Verify connectivity between the management PC and R1.

Be sure to configure the default gateway on the management PC to allow for connectivity.

Step 3: Enable security.

While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

a. Create an ACL that allows only the Management PC to access the router.

```
R1(config)#access-list 101 deny ip any 192.168.20.0  0.0.0.255
R1(config)#access-list 101 permit ip any any
R1(config)#access-list 102 permit ip host 192.168.20.50 any
```

b. Apply the ACL to the proper interface(s).

```
R1(config-subif)#interface g0/0.1
R1(config-subif)#ip access-group 101 in
R1(config-subif)#interface g0/0.2
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.2, changed state to up

R1(config-subif)#ip access-group 101 in
R1(config-subif)#line vty 0 4
R1(config-line)#access-class 102 in
```

Step 4: Verify security.

a. Verify only the Management PC can access the router.
   Use SSH to access R1 with username SSHadmin and password ciscosshpa55.
   PC> ssh -l SSHadmin 192.168.20.100
b. From the management PC, ping SW-A, SW-B, and R1.
   The pings should have been successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.
c. From D1, ping the management PC.

The ping should have failed because for a device within a different VLAN to successfully ping a device within VLAN20, it must be routed. The router has an ACL that prevents all packets from accessing the 192.168.20.0 network.

Step 5: Check results.

Your completion percentage should be 100%. Click Check Results to view feedback and verification of which required components have been completed.

If all components appear to be correct and the activity still shows incomplete, it could be due to the connectivity tests that verify the ACL operation.

Script for SW-1

```
SW-1(config)#interface f0/23
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#switchport trunk native vlan 15
SW-1(config-if)#switchport nonegotiate
SW-1(config-if)#no shutdown
SW-1(config-if)#vlan 20
SW-1(config-vlan)#exit
SW-1(config)#interface vlan 20
SW-1(config-if)#ip address 192.168.20.3 255.255.255.0
```

Script for SW-2

```
SW-2(config)#interface f0/23
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#switchport trunk native vlan 15
SW-2(config-if)#switchport nonegotiate
SW-2(config-if)#no shutdown
SW-2(config-if)#vlan 20
SW-2(config-vlan)#exit
SW-2(config)#interface vlan 20
SW-2(config-if)#ip address 192.168.20.4 255.255.255.0
```

Script for SW-A

```
SW-A(config)#vlan 20
SW-A(config-vlan)#exit
SW-A(config)#interface vlan 20
SW-A(config-if)#ip address 192.168.20.1 255.255.255.0
SW-A(config-if)#interface f0/1
SW-A(config-if)#switchport access vlan 20
SW-A(config-if)#no shutdown
```

Script for SW-B

```
SW-B(config)#vlan 20
SW-B(config-vlan)#exit
SW-B(config)#interface vlan 20
SW-B(config-if)#ip address 192.168.20.2 255.255.255.0
```

Script for Central

```
Central(config)#vlan 20
Central(config-vlan)#exit
Central(config)#interface vlan 20
Central(config-if)#ip address 192.168.20.5 255255.255.0
Central(config-if)#ip address 192.168.20.5 255.255.255.0
```

Script for R1

```
R1(config)#interface GigabitEthernet0/0.1
R1(config-subif)#ip access-group 101 in
R1(config-subif)#interface GigabitEthernet0/0.2
R1(config-subif)#ip access-group 101 in
R1(config-subif)#interface g0/0.3
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.100 255.255.255.0
R1(config-subif)#access-list 101 deny ip any 192.168.20.0 0.0.0.255
R1(config)#access-list 101 permit ip any any
R1(config)#access-list 102 permit ip host 192.168.20.50 any
R1(config)#line vty 0 4
R1(config-line)#access-class 102 in
```