Lab 09

Layer 2 Security and Layer 2 VLAN Security

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

9.1 Layer 2 Security

9.1.1 Objective

The Objectives of this lab are:

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable port security to prevent CAM table overflow attacks.

9.1.2 Background/Scenario

There have been a number of attacks on the network recently. For this reason, the network administrator has assigned you the task of configuring Layer 2 security.

For optimum performance and security, the administrator would like to ensure that the root bridge is the 3560 Central switch. To prevent spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. To prevent against CAM table overflow attacks, the network administrator has decided to configure port security to limit the number of MAC addresses each switch port can learn. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown.

All switch devices have been preconfigured with the following

- Console password: **ciscoconpa55**
- Enable password: **ciscoenpa55**
- SSH username and password: **SSHadmin/ ciscosshpa55**

9.1.3 Topology

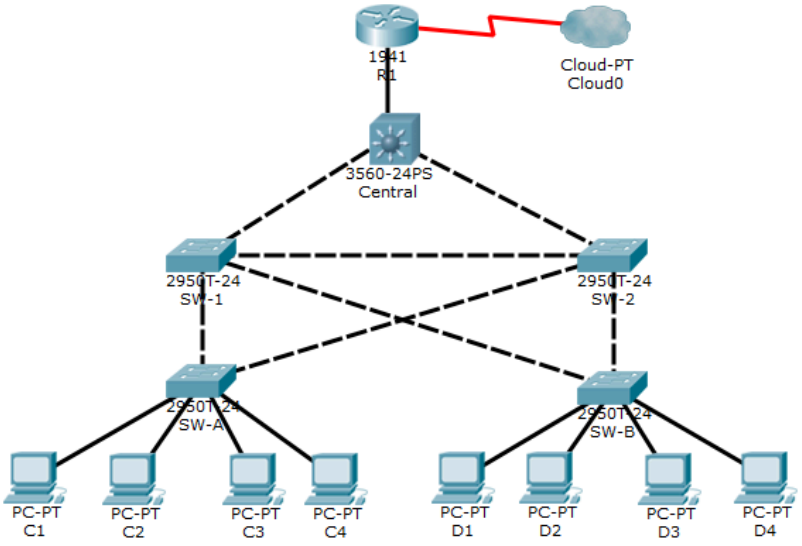


Figure 1: Topology

Task 1.1: Configure Root Bridge

1. Determine the current root bridge

   From Central, issue the **show spanning-tree** command to determine the current root bridge, to see the ports in use, and to see their status.

   Which switch is the current root bridge?

```
Central>
Central>show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0009.7C61.9058
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D31C.634C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
Fa0/1            Desg FWD 19        128.1    P2p
```

SW-1

2. Assign Central as the primary root bridge.

Using the **spanning-tree vlan 1 root primary** command and assign **Central** as the root bridge.

```
Central(config)#spanning-tree vlan 1 root primary
```

3. Assign SW-1 as a secondary root bridge.

   Assign **SW-1** as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command.

```
SW-1(config)#spanning-tree vlan 1 root secondary
```

4. Verify the spanning-tree configuration

   Issue the **show spanning-tree** command to verify that **Central** is the root bridge.

   Which switch is the current root bridge?

```
Central#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00D0.D31C.634C
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     00D0.D31C.634C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
Fa0/1            Desg FWD 19        128.1    P2p
```

Current root is Central

Task 1.2: Protect Against STP Attacks

Secure the STP parameters to prevent STP manipulation attacks

1. Enable PortFast on all access ports.

   PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the **SW-A** and **SW-B,** use the **spanning-tree portfast** command.

```
SW-A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)#interface range f0/1 - 4
SW-A(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.
%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 FastEthernet0/3 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 FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
```

```
SW-B#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)#interface range f0/1 - 4
SW-B(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.
%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 FastEthernet0/3 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 FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
```

2. Enable BPDU guard on all access ports.

   BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU guard on **SW-A** and **SW-B** access ports.

```
SW-A(config-if-range)#spanning-tree bpduguard enable
SW-B(config-if-range)#spanning-tree bpduguard enable
```

   Note: Spanning-tree BPDU guard can be enabled on each individual port using the **spanning-tree bpduguard enable** command in interface configuration mode or the **spanning-tree portfast bpduguard default** command in global configuration mode. For grading purposes in this activity, please use the **spanning-tree bpduguard enable** command.

3. Enable root guard

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the **show spanning-tree** command to determine the location of the root port on each switch.

On **SW-1**, enable root guard on ports F0/23 and F0/24. On **SW-2**, enable root guard on ports F0/23 and F0/24.

```
SW-1(config-if-range)#interface range f0/23 - 24
SW-1(config-if-range)#spanning-tree guard root
SW-2(config)#interface range f0/23- 24
SW-2(config-if-range)#spanning-tree guard rot
                                           ^
% Invalid input detected at '^' marker.

SW-2(config-if-range)#spanning-tree guard root
```

Task 1.3: Configure Port Security and Disable Unused Ports

1. Configure basic port security on all ports connected to host devices.

   This procedure should be performed on all access ports on **SW-A** and **SW-B**. Set the maximum number of learned MAC addresses to **2**, allow the MAC address to be learned dynamically, and set the violation to **shutdown**.

   Note: A switchport must be configured as an access port to enable port security.

```
SW-A(config)#interface range f0/1 -22
SW-A(config-if-range)#switchport mode access
SW-A(config-if-range)#switchport port-security
SW-A(config-if-range)#switchport port-security maximum 2
SW-A(config-if-range)#switchport port-security violation shutdown
SW-A(config-if-range)#switchport port-security mac-address sticky
SW-B(config-if-range)#interface range f0/1 - 22
SW-B(config-if-range)#switchport mode access
SW-B(config-if-range)#switchport port-security
SW-B(config-if-range)#switchport port-security maximum 2
SW-B(config-if-range)#switchport port-security violation shutdown
SW-B(config-if-range)#switchport port-security mac-address sticky
```

Why is port security not enabled on ports that are connected to other switch devices?

When ports on switch devices connect to other switches, they often accumulate numerous MAC addresses for a single port. Limiting the number of MAC addresses that these ports can learn can

greatly affect network functionality.

Essentially, each switch port maintains a list of MAC addresses it learns, which helps it direct traffic correctly within the network. If the number of addresses that can be learned is restricted, the switch may struggle to properly manage network traffic. This can lead to issues like increased packet loss, inefficient routing, and slower network performance, especially in environments with many devices. Consequently, it's crucial to carefully manage these limits to ensure optimal network operations

2. Verify port security.

a. On **SW-A**, issue the command **show port-security interface f0/1** to verify that port security has been configured.

```
SW-A# show port-security interface f0/1
```

```
SW-A#show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

b. Ping from C1 to C2 and issue the command **show port-security interface f0/1** again to verify that the switch has learned the MAC address for **C1**.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.11

Pinging 10.1.1.11 with 32 bytes of data:

Reply from 10.1.1.11: bytes=32 time<1ms TTL=128
Reply from 10.1.1.11: bytes=32 time<1ms TTL=128
Reply from 10.1.1.11: bytes=32 time<1ms TTL=128
Reply from 10.1.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
SW-A#show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0060.3E81.4647:1
Security Violation Count   : 0
```

3. Disable unused ports.

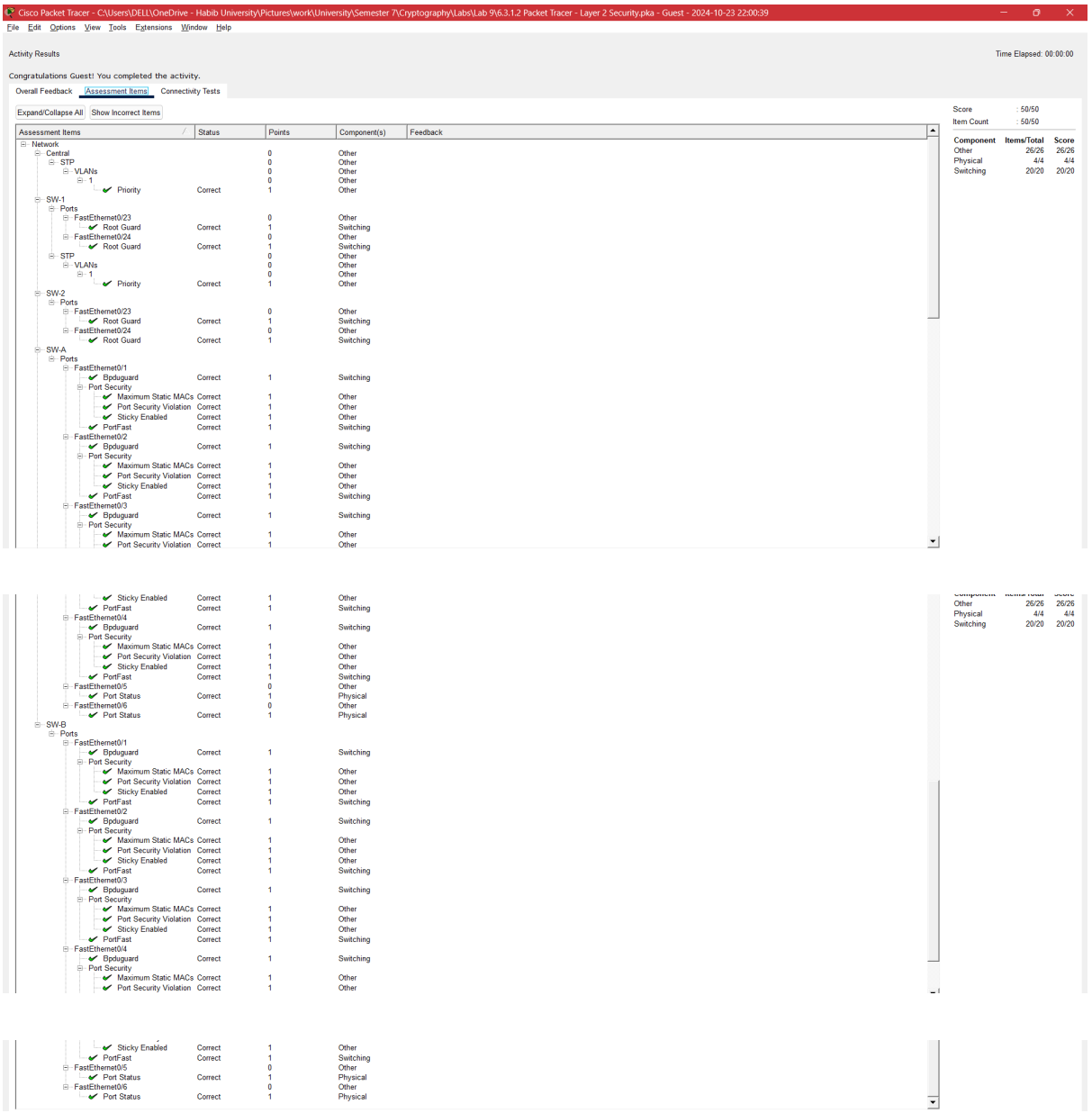
   Disable all ports that are currently unused.

```
SW-A(config)#interface range f0/5 - 22
SW-A(config-if-range)#shutdown

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

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

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

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

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
```

```
SW-B(config)#interface range f0/5 - 22
SW-B(config-if-range)#shutdown

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

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

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

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

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
```

4. Check Results.

PROOF OF COMPLETION


Cisco Packet Tracer - C:\Users\DELL\OneDrive - Habib University\Pictures\work\University\Semester 7\Cryptography\Labs\Lab 9\6.3.1.2 Packet Tracer - Layer 2 Security.pka - Guest - 2024-10-23 22:00:39
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 00:00:00
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Score : 50/50
Item Count : 50/50
Component Items/Total Score
Other 26/26 26/26
Physical 4/4 4/4
Switching 20/20 20/20
Assessment Items
Status
Points
Component(s)
Feedback
Network
Central
STP
VLANs
1
Priority Correct 1 Other
SW-1
Ports
FastEthernet0/23
Root Guard Correct 1 Switching
FastEthernet0/24
Root Guard Correct 1 Switching
SW-2
SW-A
FastEthernet0/1
Bpduguard Correct 1 Switching
Port Security
Maximum Static MACs Correct 1 Other
Port Security Violation Correct 1 Other
Sticky Enabled Correct 1 Other
PortFast Correct 1 Switching
FastEthernet0/2
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
Port Status Correct 1 Physical
FastEthernet0/6
SW-B

9.2 Layer 2 VLAN Security – Optional

8.2.1 Objectives:

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

9.2.2 Background/Scenario:

A company's network is currently set up using two separate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15. A network administrator wants to add a redundant link between switch SW-1 and SW-2. The link must have trunking enabled and all security requirements should be in place.

In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to enable the management PC to connect to all switches and the router but does not want any other devices to connect to the management PC or the switches. The administrator would like to create a new VLAN 20 for management purposes.

All devices have been preconfigured with:

- Console password: **ciscoconpa55**
- Enable password: **ciscoenpa55**
- SSH username and password: **SSHadmin/ ciscosshpa55**

8.2.3 Topology:

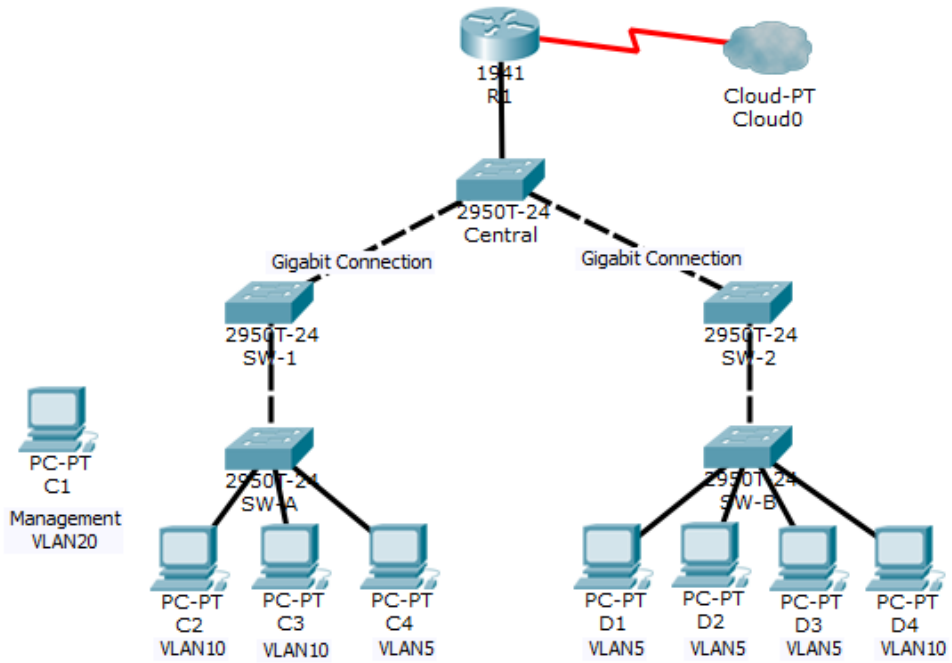


Figure 2

Task 2.1: Verify Connectivity

1. Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).
2. Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5)

Note: If using the simple PDU GUI Packet, be sure to ping twice to allow for ARP

Task 2.2: Create a Redundant Link Between SW-1 and SW-2

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**.

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

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to down
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)#
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up
```

Task 2.3: 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.

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

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

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**

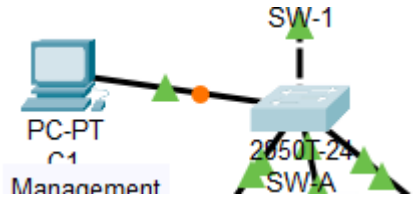
```
Central(config)#vlan 20
Central(config-vlan)#exit

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
```

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
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

%LINEPROTO-5-UPDOWN: Line protocol on 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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
ip address 192.168.20.5 255.255.255.0
```

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.



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

SW-A(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

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**

Task 2.4: Enable VLAN 20 as a Management VLAN

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)#ip address 192.168.20.100 255.255.255.0
```

2. Verify connectivity between the management PC and R1

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

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 192.168.20.0 0.0.0.255
% Incomplete command.
R1(config)#access-list 101 deny ip 192.168.20.0 0.0.0.255
R1(config)#access-list 101 deny ip 192.168.20.0 0.0.0.255
R1(config)#access-list 101 deny ip 192.168.20.0 0.0.0.255
R1(config)#access-list 101 deny ip 192.168.20.0 0.0.0.255
% Incomplete command.
R1(config)#access-list 102 permit ip host 192.168.20.50
% Incomplete command.
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
R1(config)#interface g0/0.1
R1(config-subif)#ip access-group 101 in
R1(config-subif)#interface g0/0.2
R1(config-subif)#ip access-group 101 in
R1(config-subif)#line vty 0 4
R1(config-line)#access-class 102 in
```

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

Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

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. Were the pings successful? Explain.

c. From D1, ping the management PC. Were the pings successful? Explain

5. Check results

Score	: 27/28
Item Count	: 27/28

Component	Items/Total	Score
Ip	7/7	7/7
Other	7/7	7/7
Physical	1/1	1/1
Switching	10/10	10/10
Connectivity		
Connectivity Tests	2/3	2/3

Assessment Rubric
Lab 09
Layer 2 Security and Layer 2 VLAN Security

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

Points Distribution

Task No.	**LR 2 Simulation**	**LR5 Results/Plots**	**LR9 Report**
Task 1.1	10	10	
Task 1.2	25	-	
Task 1.3	25	10	
Task 2.1	-	-	
Task 2.2	-	-	
Task 2.3	-	-	
Task 2.4	-	-	
Total	/60	/20	/10
CLO Mapped	CLO 2	CLO 2	CLO2

Affective Domain Rubric		**Points**	**CLO Mapped**
AR 7	Report Submission	/10	CLO 2

CLO	**Total Points**	**Points Obtained**
2	100	
Total	**100**	

For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.

Lab Evaluation Assessment Rubric

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3:Good Points 3	Level 4:Exemplary Points 4
LR2	**Program/Code / Simulation Model/ Network Model**	Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software.	Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software.	Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine.	Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software.
LR5	**Results & Plots**	Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner.	Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear.	All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing.	Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic.
LR9	**Report**	All the in-lab tasks are not included in report and / or the report is submitted too late.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date.	Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.