School of Computer Science and Information Technology

Department of Computer Science and Information Technology

Semester: IV
Specialisation: Internet of Things (E)

23BCA4VC02: Network Administration

Activity 2

VLAN Hopping and Defence Setup

(Simulation on CISCO Packet Tracer)

Date of Submission: 21-04-2025

Submitted by:
Name: Dhruvil Vaghasiya
Reg No./USN No: 23BCAR0319
Signature:

Faculty In-Charge:
Mr. Sahabzada Betab Badar

JGI JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

CERTIFICATE

This is to certify that **Dhruvil Vaghasiya** has satisfactorily completed activity prescribed by JAIN (Deemed to be University) for the fourth semester degree course in the year 2024-2025.

Sl. No	CRITERIA	MARKS	MARKS OBTAINED
1	On-time Submission	5	
2	Presentation Skill	10	
3	Communication Skill	10	
4	Content with example program	15	
5	Documentation	10	
	Total	50	
	Convert	15	

MARKS	
MAX	OBTAINED
15	

Signature of the Student Signature of the Faculty

Date of Submission: 21 April, 2025

INDEX

—

1. INTRODUCTION

Virtual Local Area Networks (VLANs) are very useful in today's networks. They help network administrators like me to separate one big network into smaller, manageable parts. Even if all devices are connected to the same switch, VLANs allow me to keep traffic separated by department or purpose. This setup improves the speed and security of the network. But, just like anything in networking, VLANs also come with their own risks. One of the major threats I learned about is called VLAN Hopping. In this type of attack, a hacker can try to get into other VLANs and see private data, even when they're not supposed to.

There are mainly two ways attackers perform VLAN Hopping. The first is called Switch Spoofing, where the attacker pretends their device is a switch and tricks the actual switch into creating a trunk connection. This gives them access to all VLANs on that trunk. The second method is Double Tagging, where the attacker adds two VLAN tags to their message. The first switch removes the first tag and forwards the message based on the second one, sending it to the wrong VLAN.

For this project, I designed a secure network using Cisco Packet Tracer. The goal was to show how I can set up safe VLANs and also allow them to communicate through Inter-VLAN Routing. To do this, I used a method called Router-on-a-Stick, where I used only one physical link between the switch and router, but made multiple virtual interfaces (called subinterfaces) on the router. Each subinterface handled a different VLAN.

To prevent VLAN Hopping, I applied many security techniques. I turned off automatic trunk creation by disabling DTP. I set a unique number for the native VLAN to make sure double tagging won't work. I used port security so that only specific computers can connect to each port. I also shut down all the ports that are not in use to reduce the chances of attacks.

2. STEP BY STEP, IMPLIMENTATION PROCESS

Step 1: Add and Connect Devices

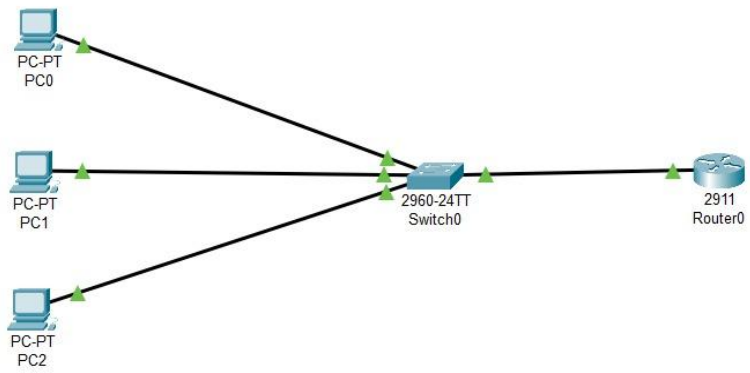
Devices Used:

- 1 Router (Cisco 2911)
- 1 Switch (Cisco 2960)
- 3 PCs (PC0, PC1, PC2)

Connections:

- PC0 → Switch FastEthernet0/1
- PC1 → Switch FastEthernet0/2
- PC2 → Switch FastEthernet0/3
- Switch GigabitEthernet0/1 → Router GigabitEthernet0/0

Use straight-through cables for all connections.



Step 2: Configure VLANs on the Switch

Switch> enable
Switch# config t
Switch(config)# vlan 10
Switch(config-vlan)# name User_VLAN

Switch(config)# vlan 20
Switch(config-vlan)# name HR_VLAN

Switch(config)# vlan 999
Switch(config-vlan)# name Native_VLAN

```
vlan 10
 name User_VLAN
!
vlan 20
 name HR_VLAN
!
vlan 30
 name Guest_VLAN
!
vlan 999
 name Native_VLAN
```

Step 3: Assign VLANs to Ports and Secure Access

PC1 → VLAN 10:

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# exit
```

PC2 → VLAN 20:

```
Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# exit
```

PC3 → VLAN 30:

```
Switch(config)# interface FastEthernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 30
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# exit
```

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.5CAC.41C9
 spanning-tree bpduguard enable
 storm-control broadcast level 10
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0010.11AD.C68A
 spanning-tree bpduguard enable
 storm-control broadcast level 10
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 000A.418E.C1A7
 spanning-tree bpduguard enable
 storm-control broadcast level 10
!
```

Step 4 :Configure Trunk to Router (Router-on-a-Stick)

Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 999
Switch(config-if)# switchport trunk allowed vlan 10,20,30
Switch(config-if)# switchport nonegotiate
Switch(config-if)# exit

```
!
interface GigabitEthernet0/1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 switchport nonegotiate
!
```

Step 5 :Disable Unused Ports

Switch(config)# interface range FastEthernet0/10 - 24
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
Switch(config)#

```
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
```

```
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
```

Step 6 :Set VTP Mode to Transparent

Switch(config)# vtp mode transparent
Switch(config)#exit

```
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
```

Step 7 :Router Configuration (Router-on-a-Stick)

Router(config)# interface GigabitEthernet0/0.10
Router(config-if)# encapsulation dot1Q 10
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# exit

Router(config)# interface GigabitEthernet0/0.20
Router(config-if)# encapsulation dot1Q 20
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config-if)# exit

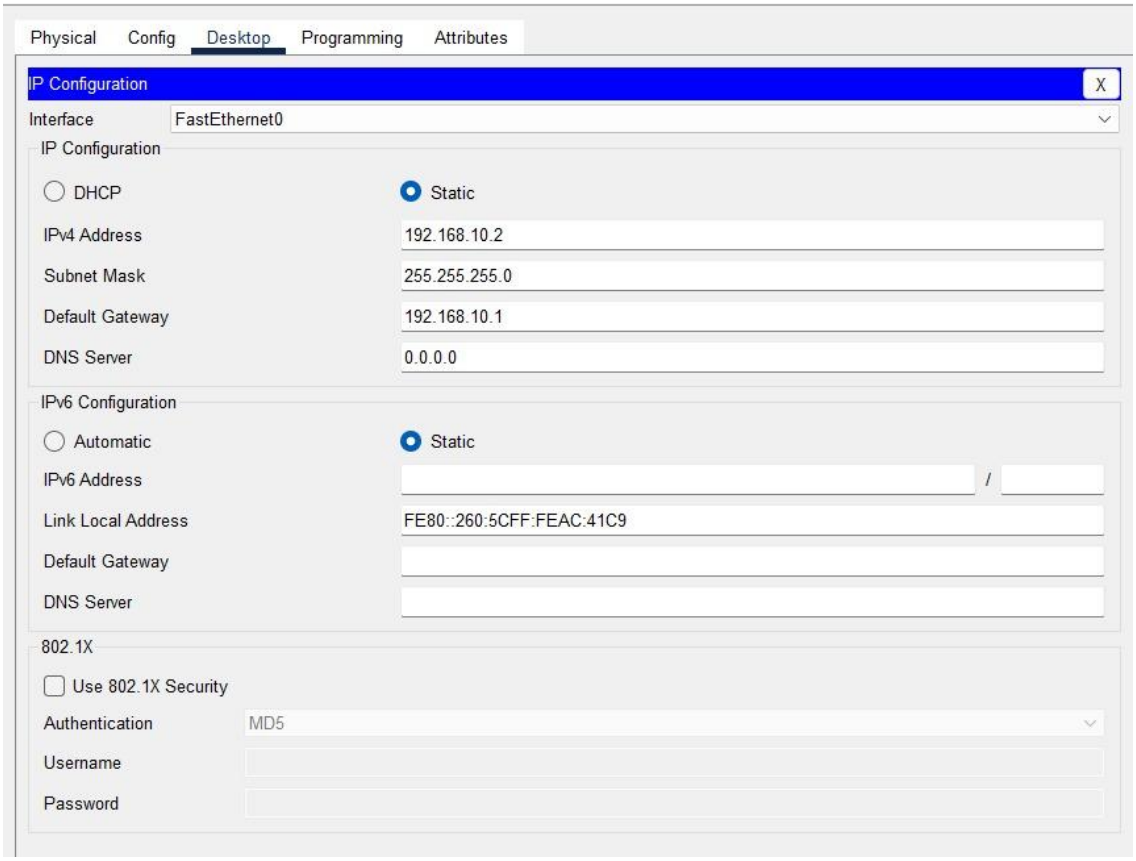
Router(config)# interface GigabitEthernet0/0.30
Router(config-if)# encapsulation dot1Q 30
Router(config-if)# ip address 192.168.30.1 255.255.255.0
Router(config-if)# exit

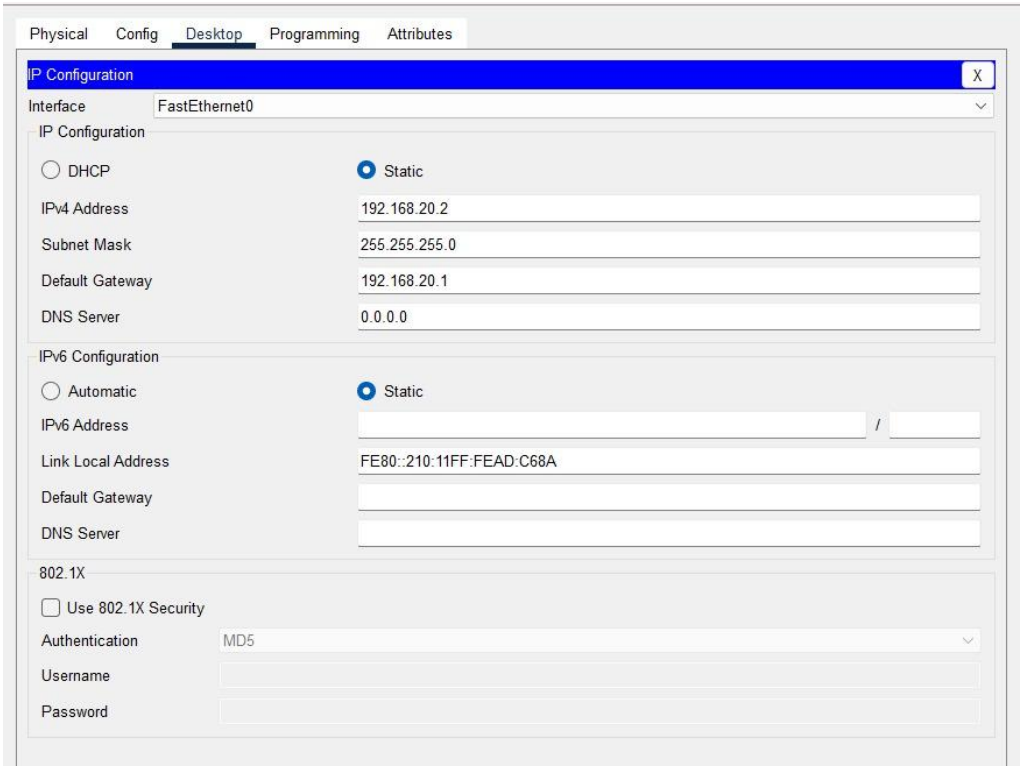
Router(config)# interface GigabitEthernet0/0
Router(config-if)# no shutdown
Router(config-if)# exit

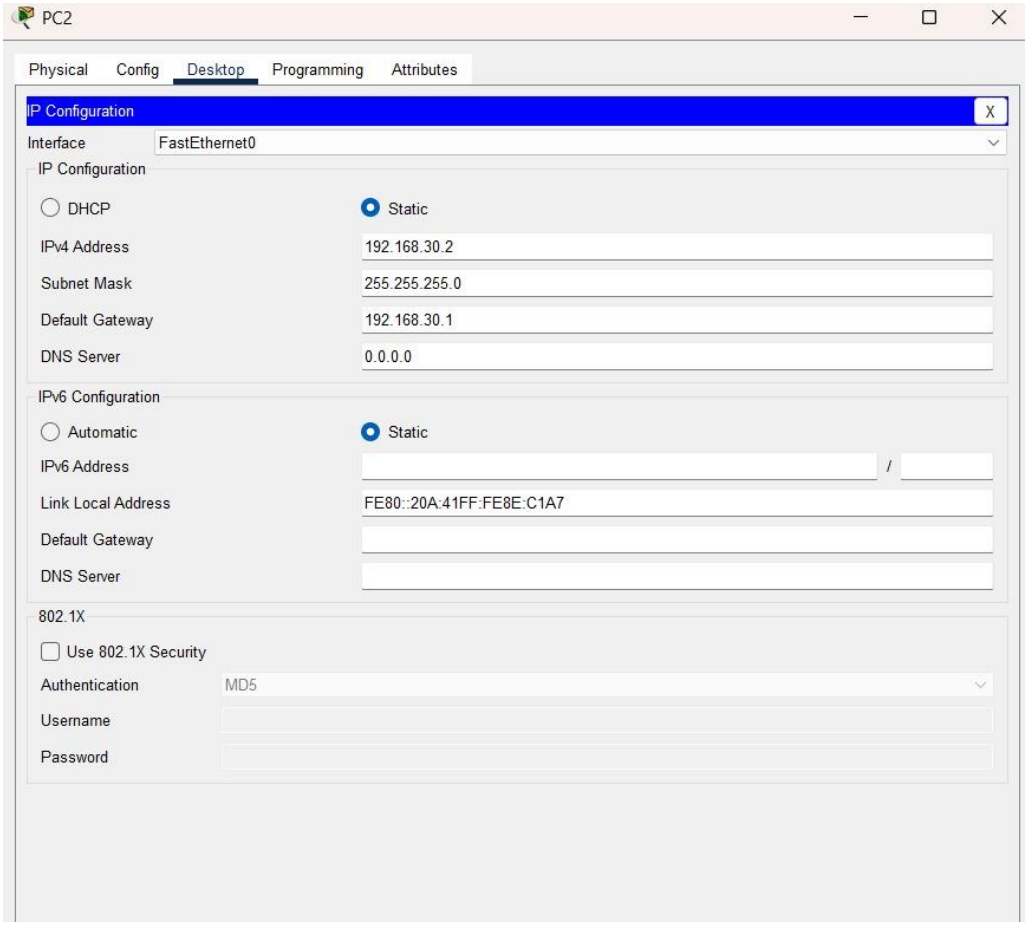
```
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
```

Step 8 :End Devices IP Configuration

Device	VLAN	IP Address	Subnet Mask	Default Gateway
PC0	10	192.168.10.2	255.255.255.0	192.168.10.1
PC1	20	192.168.20.2	255.255.255.0	192.168.20.1
PC2	30	192.168.30.2	255.255.255.0	192.168.30.1




Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.20.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.20.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::210:11FF:FEAD:C68A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.30.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20A:41FF:FE8E:C1A7
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password

3. **Verification Steps**

1. VLAN Verification:

To confirm that all VLANs (10, 20, 30, and 999) are correctly created and assigned to the appropriate access ports.

Command:
Switch# show vlan brief

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/2
10   User_VLAN                         active    Fa0/1
20   HR_VLAN                           active    Fa0/2
30   Guest_VLAN                        active    Fa0/3
999  Native_VLAN                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

2. Trunking Verification:

To verify that the trunk port (GigabitEthernet0/1) is configured correctly and allows VLANs 10, 20, and 30, with VLAN 999 as the native VLAN.

Command:
Switch# show interfaces trunk

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      999

Port        Vlans allowed on trunk
Gig0/1      10,20,30

Port        Vlans allowed and active in management domain
Gig0/1      10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20,30
```

3. Port Security Verification:

To confirm that port security is enabled on access ports (F0/1, F0/2, F0/3), with sticky MAC addresses and "restrict" as the violation mode.

Command:
Switch# show port-security

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-------------------------------------------------------------------------
        Fa0/1        1          1                0         Restrict
        Fa0/2        1          1                0         Restrict
        Fa0/3        1          1                0         Restrict
```

4. Router Interface Verification:

To check that sub-interfaces are up and correctly configured with IP addresses for each VLAN.

Command:
Router# show ip interface brief

```
Router>enable
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

5. Routing Table Verification:

To ensure that all VLAN networks are visible and routable in the router's routing table.

Command:
Router# show ip route

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0.30
```

4. Conclusion

Through this project, I was able to implement VLANs and inter-VLAN routing using the Router-on-a-Stick method, which helped me understand how network segmentation improves both performance and security. By assigning specific VLANs to different departments—User (VLAN 10), HR (VLAN 20), and Guest (VLAN 30)—I created separate broadcast domains that reduced unnecessary traffic and improved organization within the network.

I configured a router with sub-interfaces to enable communication between VLANs, which allowed devices in different VLANs to exchange data efficiently. This method proved to be both cost-effective and scalable, which is essential for real-world enterprise networks.

One of the key aspects of this project was implementing VLAN hopping prevention techniques. I changed the native VLAN to an unused one (VLAN 999), disabled DTP using switchport nonegotiate, and applied port security to restrict unauthorized access. I also enabled BPDU Guard to protect against rogue switches, shut down all unused ports to reduce vulnerabilities, and set the VTP mode to transparent to avoid unintentional VLAN changes from external devices.

To verify my setup, I used various commands like show vlan brief, show interfaces trunk, show port-security, and show ip route. These helped me confirm that the switch and router configurations were working correctly. I also performed ping tests between PCs in different VLANs, and the successful replies confirmed that inter-VLAN routing was functioning as expected.

5. References

- https://networklessons.com/cisco/ccnp-switch/vlan-hopping
- https://www.techtarget.com/searchsecurity/definition/VLAN-hopping