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

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

Fake IP Phone Attack

(Simulation on CISCO Packet Tracer)

Date of Submission: 21-04-2025

Submitted by:
Name: Deep Vaghasiya
Reg No./USN No: 23BCAR0316
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 **Deep 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

In modern enterprise networks, Voice over IP (VoIP) systems are widely used to handle communication through IP Phones. These systems often utilize a dedicated Voice VLAN to ensure quality of service (QoS), prioritize voice traffic, and isolate it from regular data traffic. While this setup provides better network performance and organization, it also introduces potential vulnerabilities if not properly secured. One such vulnerability is the Fake IP Phone Attack, where an attacker tries to mimic an IP phone to gain unauthorized access to the Voice VLAN.

The Voice VLAN, typically configured alongside a data VLAN on the same access port, allows IP phones to communicate over a separate subnet with higher priority. However, this also opens a door for malicious devices to attempt VLAN hopping or spoof their identity to pose as IP phones. If successful, attackers can intercept sensitive voice traffic, disrupt communications, or launch further attacks inside the voice network. This highlights the critical importance of implementing strong access control and security measures on switch ports.

In this simulation using Cisco Packet Tracer, the objective is to demonstrate how a regular PC, connected to a data VLAN, can be configured to impersonate an IP phone and gain access to the Voice VLAN. This is achieved by manually assigning an IP address from the voice subnet to the PC and altering the switch configuration to treat the port as one supporting both data and voice VLANs. The result is a simple yet effective method of bypassing VLAN isolation.

The simulation is designed to help understand the weaknesses in typical switch configurations and how easily an attacker can exploit them if basic security is overlooked. Although this attack may not be highly advanced, it represents a realistic threat, especially in environments where switch ports are left misconfigured or unsecured. It serves as a valuable learning tool for recognizing poor VLAN deployment practices.

Furthermore, the attack scenario provides a foundation for exploring defensive strategies such as enabling DHCP snooping, port security, and Dynamic ARP Inspection (DAI). These techniques can significantly reduce the chances of VLAN hopping or unauthorized access by ensuring that only legitimate devices receive IP addresses and participate in VLAN communications.

2. STEP BY STEP, IMPLIMENTATION PROCESS

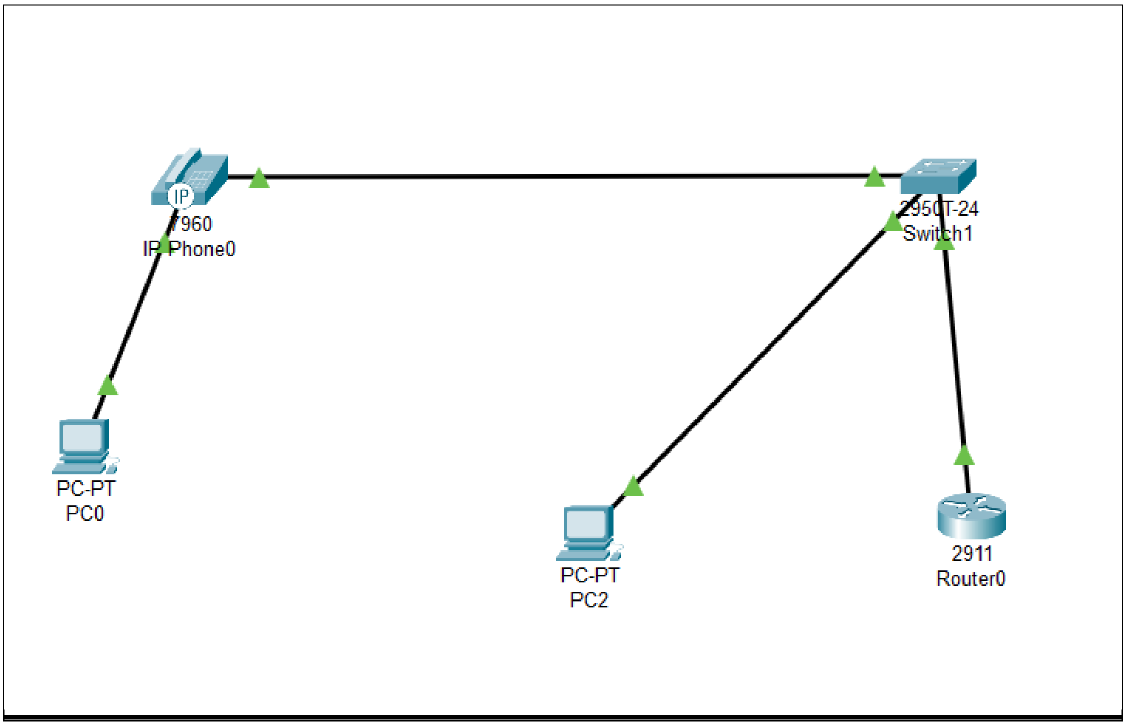
Step 1: Add and Connect Devices

Devices Used:

- 1 Router (Cisco 2901)
- 1 Switch (Cisco 2960)
- 1 PC (PC1)
- 1 IP Phone (Cisco 7960)
- Straight-through cables as needed

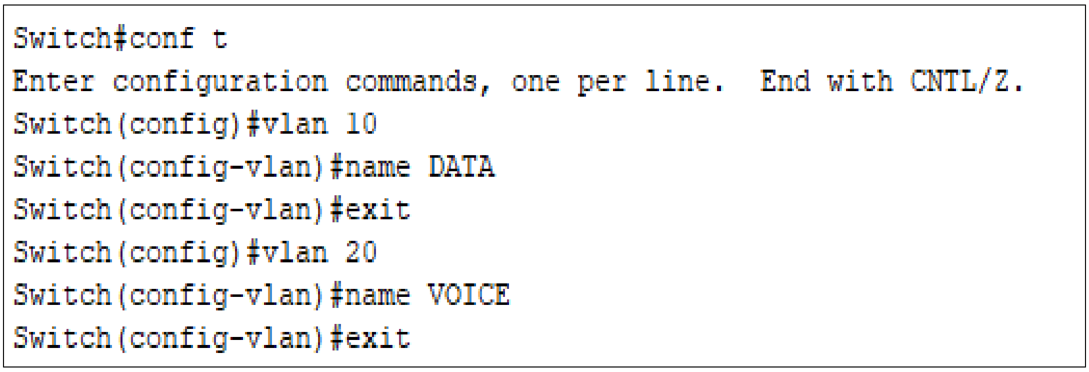
Connections:

- Router Gig0/0 → Switch Gig0/1
- PC1 → Switch FastEthernet0/2
- IP Phone → Switch FastEthernet0/1



Step 2: Configure VLANs on the Switch

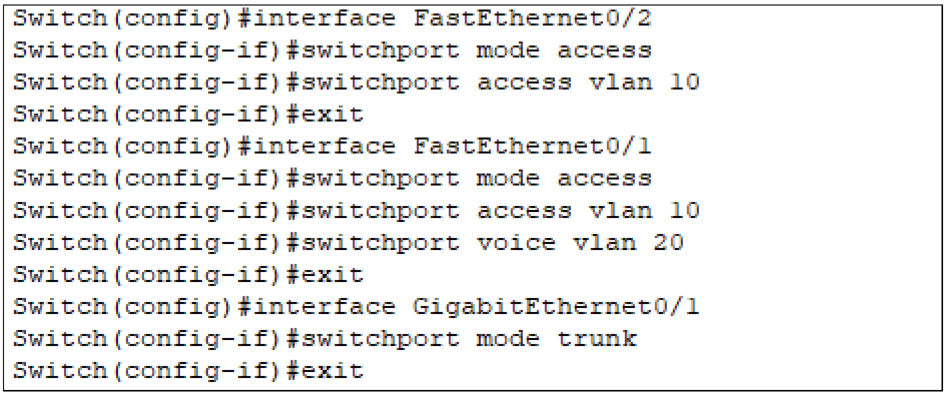
```
Switch> enable
Switch# configure terminal

Switch(config)# vlan 10
Switch(config-vlan)# name DATA
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name VOICE
Switch(config-vlan)# exit
```



```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name DATA
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VOICE
Switch(config-vlan)#exit
```

Step 3: Assign VLANs to Ports

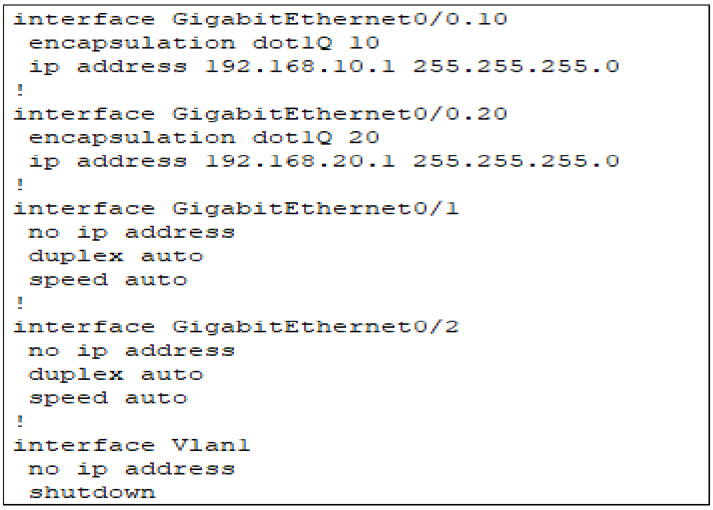
```
Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport voice vlan 20
Switch(config-if)# exit

Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```



```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 20
Switch(config-if)#exit
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Step 4 : Configure Router Sub-Interfaces (Router-on-a-Stick)

```
Router> enable
Router# configure terminal

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
Router(config-if)# no shutdown
Router(config-if)# exit
```



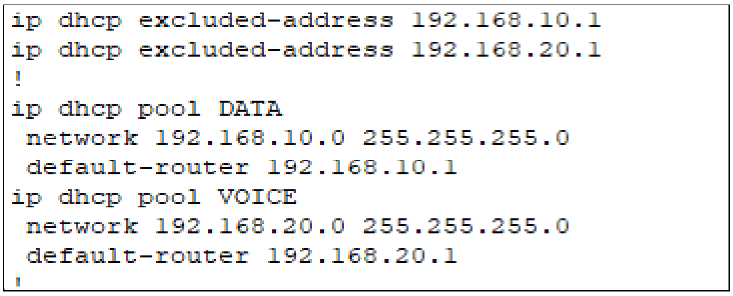
```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no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

Step 5 : Configure DHCP on Router

Router(config)# ip dhcp excluded-address 192.168.10.1
Router(config)# ip dhcp excluded-address 192.168.20.1

Router(config)# ip dhcp pool DATA
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# exit

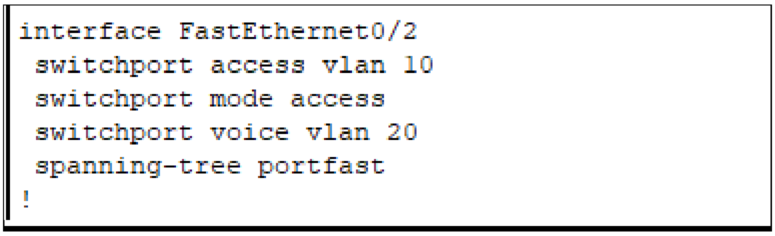
Router(config)# ip dhcp pool VOICE
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# exit



```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool DATA
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
ip dhcp pool VOICE
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
!
```

Step 6 : Simulate the Fake IP Phone Attack

Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport voice vlan 20
Switch(config-if)# spanning-tree portfast
Switch(config-if)# exit



```
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 20
 spanning-tree portfast
!
```

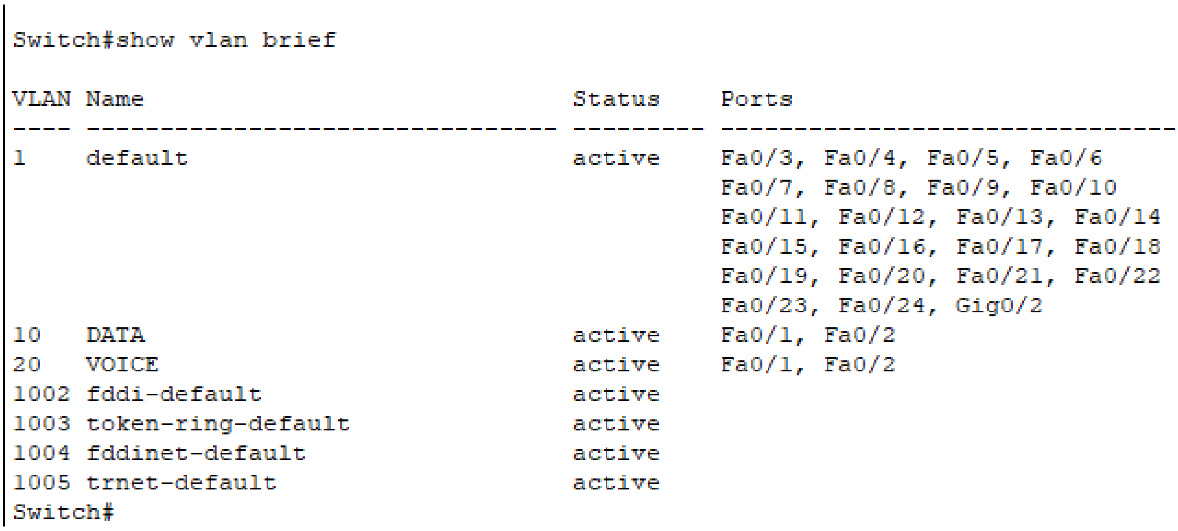
3. Verification Steps

1. VLAN Verification:

To ensure that VLAN 10 (DATA) and VLAN 20 (VOICE) are created and assigned to the correct interfaces:

- Fa0/1: Access VLAN 10, Voice VLAN 20
- Fa0/2: Access VLAN 10 (modified to include Voice VLAN 20 in the attack simulation)

Command:
Switch# show vlan brief

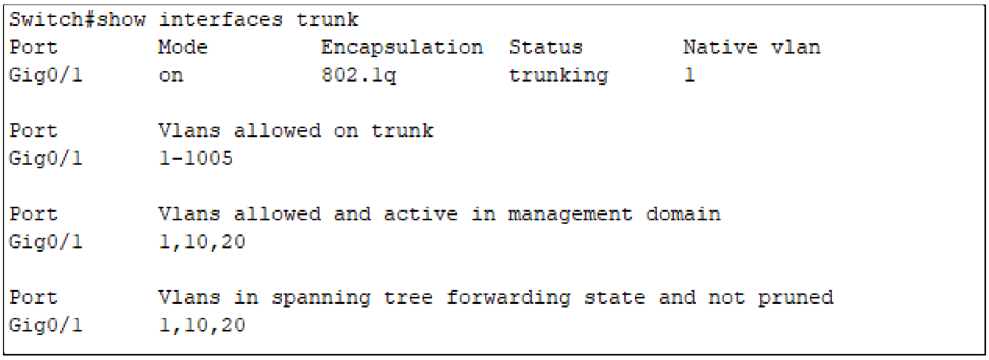


```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, 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   DATA                             active    Fa0/1, Fa0/2
20   VOICE                            active    Fa0/1, Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

2. Verify Trunk Port Configuration:

To confirm that **GigabitEthernet0/1** is correctly configured as a trunk port, allowing VLAN 10 and VLAN 20 traffic between the switch and the router.

Command:
Switch# show interfaces trunk

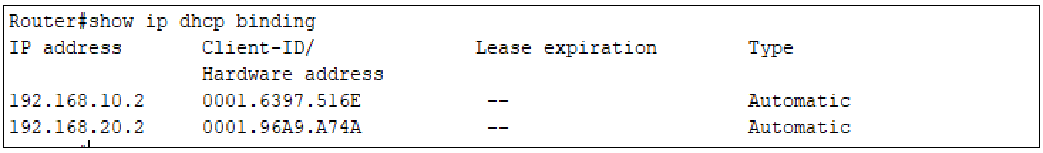


```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

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

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

3. Verify DHCP Bindings on Router:

To view the IP addresses leased to devices. If PC1 manually sets an IP in VLAN 20, it won’t appear here. But normally assigned IPs for IP Phone should be listed.

Command:
Router# show ip dhcp binding

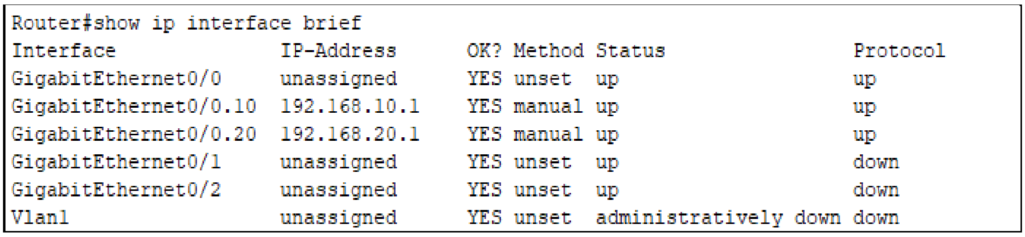


```
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.2     0001.6397.516E           --                     Automatic
192.168.20.2     0001.96A9.A74A           --                     Automatic
```

4. Router Interface Verification:

To check if sub-interfaces GigabitEthernet0/0.10 and GigabitEthernet0/0.20 are **up** and have correct IP addresses assigned.

Command:
Router# show ip interface brief

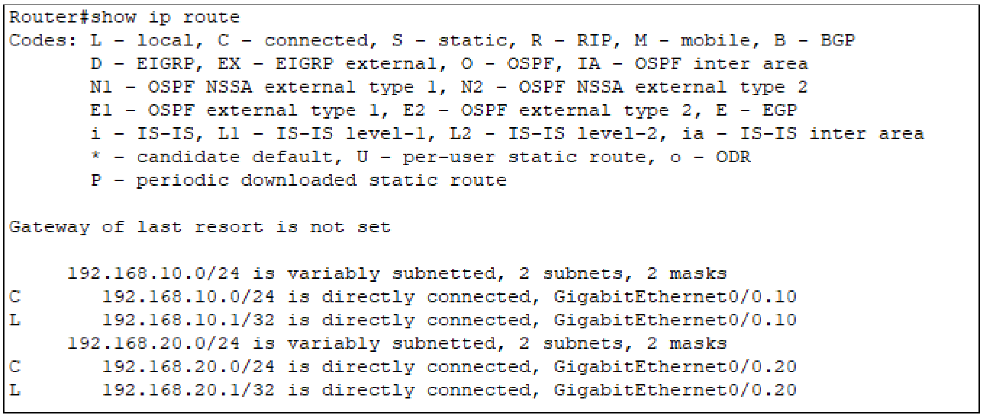


```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1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

5. Routing Table Verification:

To verify that the router can route between VLANs 10 and 20, and that the networks 192.168.10.0/24 and 192.168.20.0/24 are present in the 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
```

4. Conclusion

In this project, I successfully simulated a Fake IP Phone Attack in Cisco Packet Tracer to demonstrate how a malicious device can gain unauthorized access to the Voice VLAN (VLAN 20) by spoofing itself as an IP phone. This simulation helped me understand a critical security vulnerability that can exist in enterprise networks if access ports are not properly secured.

The setup included a typical voice and data VLAN configuration, where the IP phone was connected to a port configured for both access VLAN 10 (Data) and voice VLAN 20. I then modified the settings of a normal PC (PC1) to statically assign it an IP address from the Voice VLAN subnet. By altering the port configuration on the switch, PC1 was able to simulate an IP phone and gain access to the Voice VLAN — effectively imitating a real-world spoofing attack.

Through this attack simulation, I was able to observe how a simple configuration oversight could allow a regular PC to bypass VLAN separation and communicate with sensitive devices like IP phones. The ability to ping and interact with the Voice VLAN confirmed the success of the spoofing attempt. This reinforces the importance of robust switch security settings in protecting network segments.

To defend against such attacks, I explored and recommended preventive measures such as enabling DHCP snooping, Dynamic ARP Inspection (DAI), and applying port security to restrict unauthorized devices. These features are essential to prevent VLAN hopping, spoofing, and unauthorized DHCP usage on access ports.

5. Refrences

- https://team-sik.org/wp-content/uploads/2020/01/44conMasterDraft.pdf
- https://www.kaspersky.com/resource-center/threats/ip-spoofing