Secure a Network Using Cisco Security Features

Supervised by:- Eng Magdy Ibrahim

Presented by:-

- Alaa Esam
- Nour Shady
- Rawan Tarek
- Mohamed Ashraf
- Mohamed Waleed
- Omar Ahmed

AGENDA:–

- Introduction
- Network Design and Topology
- Basic Security Setup (Basic Configuration, Port Security)
- Access Control List (ACL)
- VLAN Configuration and Inter-VLAN Routing
- OSPF Configuration
- Advanced Security Features: DHCP Snooping, DAI, IP Source Guard
- Testing and Validation of Security Measures
- Conclusion and Recommendations
- Q&A

1. INTRODUCTION

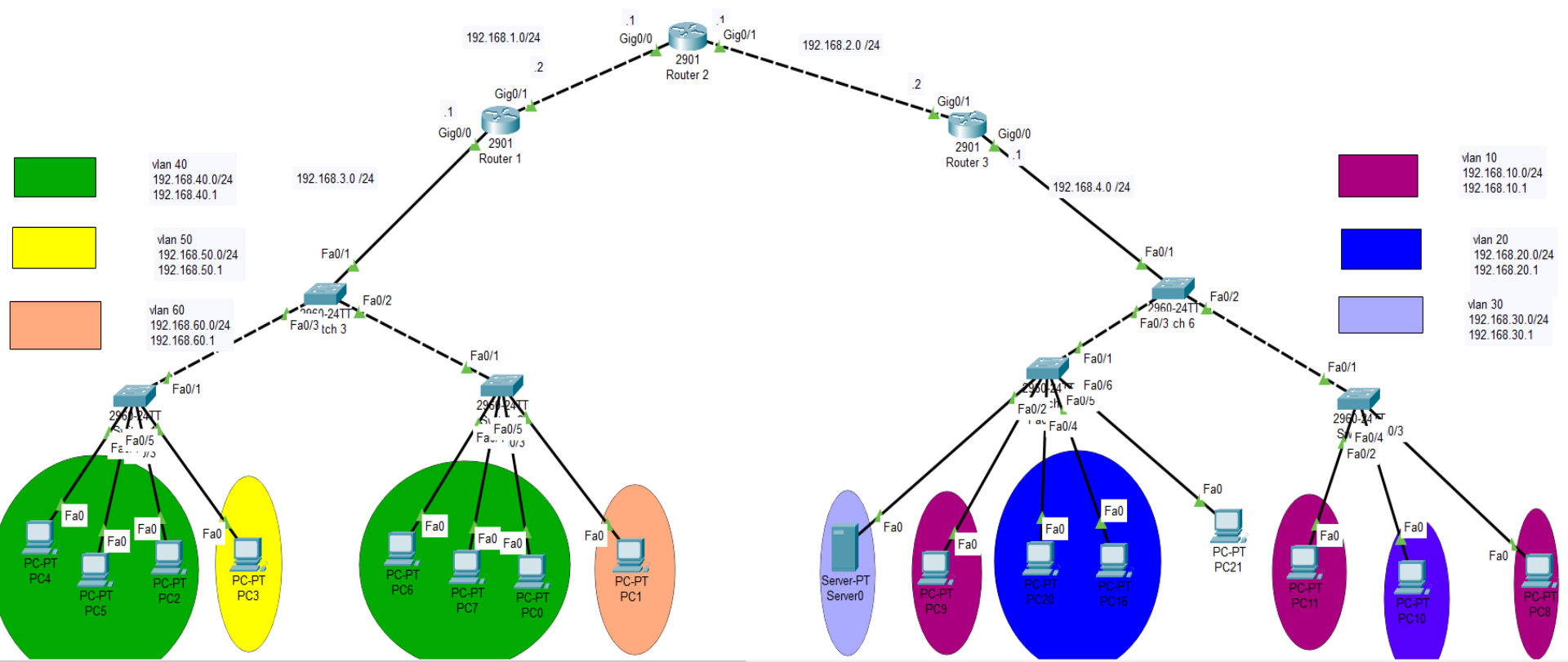
INTRODUCTION

- This project focuses on securing a medium to large-scale corporate network, where VLANs isolate different departments while ensuring secure communication. Using Cisco security features like ACLs, DHCP snooping, DAI, and IP Source Guard, the network is protected from vulnerabilities and unauthorized access.

- This presentation will cover the network design, security configurations, and how these measures improve both security and network performance.

2.
NETWORK DESIGN AND TOPOLOGY

TOPOLOGY


192.168.1.0/24
.1
Gig0/0
.1
Gig0/1
192.168.2.0 /24
.2
Gig0/1
2901
Router 2
.2
Gig0/1
.1
Gig0/0
2901
Router 1
2901
Router 3
Gig0/0
.1
192.168.3.0 /24
192.168.4.0 /24
vlan 40
192.168.40.0/24
192.168.40.1
vlan 50
192.168.50.0/24
192.168.50.1
vlan 60
192.168.60.0/24
192.168.60.1
vlan 10
192.168.10.0/24
192.168.10.1
vlan 20
192.168.20.0/24
192.168.20.1
vlan 30
192.168.30.0/24
192.168.30.1
Fa0/1
Fa0/2
Fa0/3
Fa0/4
Fa0/5
Fa0/6
Fa0
PC-PT
PC4
PC5
PC2
PC3
PC6
PC7
PC0
PC1
Server-PT
Server0
PC9
PC20
PC16
PC21
PC11
PC10
PC8

ADDRESSING TABLE

Device	Interface	IP Address	Subnet Mask
R1	G0/0	192.168.3.1	255.255.255.0
	G0/0.40	192.168.40.1	255.255.255.0
	G0/0.50	192.168.50.1	255.255.255.0
	G0/0.60	192.168.60.1	255.255.255.0
	G0/0.100	192.168.100.1	255.255.255.0
	G0/1	192.168.1.2	255.255.255.0
R2	G0/0	192.168.1.1	255.255.255.0
	G0/1	192.168.2.1	255.255.255.0
R3	G0/0	192.168.4.1	255.255.255.0
	G0/0.10	192.168.10.1	255.255.255.0
	G0/0.20	192.168.20.1	255.255.255.0
	G0/0.30	192.168.30.1	255.255.255.0
	G0/0.100	192.168.100.1	255.255.255.0
	G0/1	192.168.2.2	255.255.255.0
Server	NIC	192.168.30.25	255.255.255.0

VLAN TABLE

VLAN	Name	Interface Assigned
1	Default	S1: F0/6-24 , G0/1-2 S2: F0/6-24 , G0/1-2 S3: f0/5-24, G0/1-2 S4: F0/6-24, G0/1-2
10	Admin_VLAN	S3: F0/2 , F0/4 S4: F0/3
20	IT_VLAN	S3: F0/3 S4: F0/4 , F0/5
30	Server_VLAN	S4: F0/2
40	Engineering_VLAN	S1: f0/2-4 S2: f0/2-4
50	Marketing_VLAN	S1: F0/5
60	Finance_VLAN	S2: F0/5
100	Native	N/A

3.
BASIC SECURITY SETUP

BASIC SECURITY CONFIGURATIN

Importance of Basic Security Configurations:

- Strong Passwords: Complex combinations prevent unauthorized access.
- Encrypted Communication: Secures data from interception during transmission.
- SSH: Encrypts admin access to prevent eavesdropping.
- Service Password Encryption: Hides passwords in configuration files.
- Banner Messages: Legal notices warning unauthorized users.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret cisco
S1(config)#line console 0
S1(config-line)#password project
S1(config-line)#no exec-timeout
S1(config-line)#logging synchronous
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 14
S1(config-line)#password project
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#no ip domain-lookup
S1(config)#ip domain-name example.com
S1(config)#crypto key generate rsa
The name for the keys will be: S1.example.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#line vty 0 15
*Mar 1 0:1:32.252: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#username admin secret cisco
S1(config)#banner motd #Unauthorized access to this device is prohibited!#
S1(config)#exit
S1#copy running-config startup-config
```

PORT SECURITY

Benefits of Port Security:

- Enhanced Security: By restricting access to only authorized devices.
- Prevention of MAC Flooding Attacks: Limits the impact of potential MAC address flooding.
- Administrative Control: Provides network administrators with control over which devices can connect to the network.

```
Switch>
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/2-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------------
        Fa0/2        1           1                0         Shutdown
        Fa0/3        1           1                0         Shutdown
        Fa0/4        1           1                0         Shutdown
        Fa0/5        1           1                0         Shutdown
--------------------------------------------------------------------------
Switch#show port-security int f0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0000.0C20.5BEA:1
Security Violation Count   : 0
```

4.
ACCESS CONTROL LIST (ACL)

Access Control Lists (ACLs)

Access Control Lists (ACLs)ACLs are sets of rules that control network traffic, filtering it based on IP addresses, protocols, or ports. They enhance security by restricting access between VLANs or network segments, ensuring only authorized devices or users can communicate.

How ACLs Protect Against Internal and External Threats

- Internal Threats: ACLs limit access between internal departments (e.g., admin, IT, finance), preventing unauthorized users from accessing sensitive resources within the network.
- External Threats: ACLs block unwanted external traffic, ensuring that only trusted sources can access the network, reducing the risk of attacks like unauthorized logins or data breaches.

1- STANDARD ACL

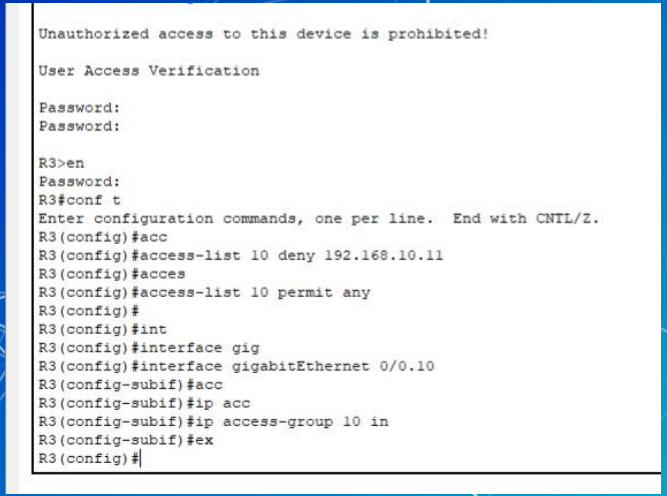
BLOCK_VLAN 40_VLAN 50

- Purpose: Prevents communication between VLAN 40 and VLAN 50.
- Explanation: Ensures that devices in VLAN 40 cannot communicate with devices in VLAN 50, isolating traffic between the two VLANs for

```
User Access Verification

Password:
Password:

R1>en
Password:
Password:
R1#
R1#
R1#
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#ip acc
R1(config)#ip access-list ext
R1(config)#ip access-list extended BLOCK_VLAN40_VLAN50
R1(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
R1(config-ext-nacl)#permit
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#ex
R1(config)#
R1(config)#int
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/0.40
R1(config-subif)#ip acc
R1(config-subif)#ip access-group BLOCK_VLAN40_VLAN50 in
R1(config-subif)#ex
R1(config)#
```

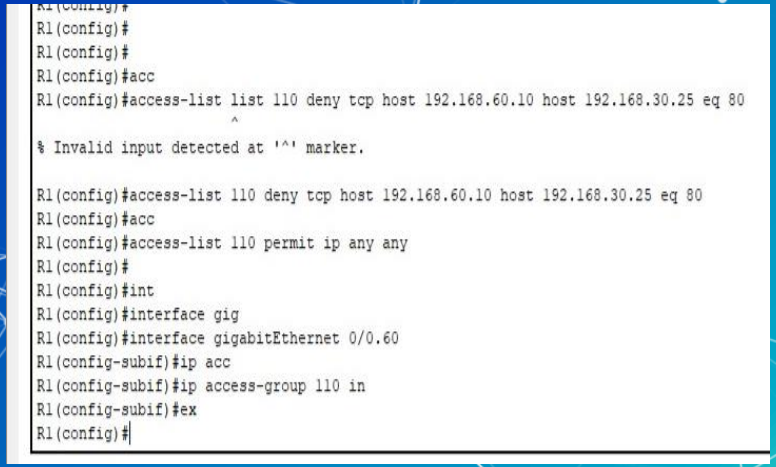
STANDARD ACLs PC 8

- Purpose: Restricts network access to only PC8.
- Explanation: Limits network access to PC8's specific IP address, ensuring no other devices can connect through this interface.



2- EXTENDED ACL

- PC1 Extended ACL (TCP)
- Purpose: Blocks PC1 from accessing web traffic (HTTP).
- Explanation: This ACL prevents PC1 from sending or receiving HTTP (web) traffic, effectively blocking access to websites, while allowing other traffic types to pass through.



5.
VLANs CONFIGURATION

VLANs

What are VLANs?

VLANs (Virtual Local Area Networks) group devices into separate networks, regardless of their physical location.

Importance of VLANs:

- Segmentation: Isolates departments (admin, IT, engineering, server, marketing, finance) to enhance security.
- Improved Security: Protects sensitive data by minimizing unauthorized access.
- Enhanced Performance: Reduces broadcast traffic, improving network efficiency.
- Simplified Management: Facilitates easier network management and policy application.
- Flexibility: Allows device mobility between VLANs without physical changes.

VLAN CONFIGURATION

```
S2>
S2>
S2>
S2>en
Password:
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 40
S2(config-vlan)#name Engineering_VLAN
S2(config-vlan)#vlan 50
S2(config-vlan)#name Marketing_VLAN
S2(config-vlan)#vlan 60
S2(config-vlan)#name Finance_VLAN
S2(config-vlan)#vlan 100
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#int f0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 40
S2(config-if)#int f0/3
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 40
S2(config-if)#int f0/4
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 40
S2(config-if)#int f0/5
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 60
S2(config-if)#int f0/1
S2(config-if)#switchport mode trunk

S2(config-if)#switchport trunk native vlan 100
S2(config-if)#switchport trunk allowed vlan 40,50,60,100
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed stat

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

```
S3>en
Password:
S3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/
S1 FastEthernet0/1 (100).

S3(config)#vlan 40
S3(config-vlan)#name Engineering_VLAN
S3(config-vlan)#vlan 50
S3(config-vlan)#name Marketing_VLAN
S3(config-vlan)#vlan 60
S3(config-vlan)#name Finance_VLAN
S3(config-vlan)#vlan 100
S3(config-vlan)#name Native
S3(config-vlan)#exit
S3(config)#int vlan 100
S3(config-if)#ip address 192.168.3.3 255.255.255.0
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.3.1
S3(config)#int f0/1
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 100
S3(config-if)#switchport trunk allowed vlan 40,50,60,100
S3(config-if)#int f0/2
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 100
S3(config-if)#switchport trunk allowed vlan 40,50,60,100
S3(config-if)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 100
S3(config-if)#switchport trunk allowed vlan 40,50,60,100
%LINK-5-CHANGED: Interface Vlan100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up
```

INTER-VLAN ROUTING

```
%Invalid hex value
R1(config)#int g0/0
R1(config-if)#no sh

R1(config-if)#int g0/0.40
R1(config-subif)#Description Default gateway for vlan 40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0.50
R1(config-subif)#Description Default gateway for vlan 50
R1(config-subif)#encapsulation dot1Q 50
R1(config-subif)#ip address 192.168.50.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0.60
R1(config-subif)#Description Default gateway for vlan 60
R1(config-subif)#encapsulation dot1Q 60
R1(config-subif)#ip address 192.168.60.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0.100
R1(config-subif)#Description Default gateway for vlan 100
R1(config-subif)#encapsulation dot1Q 100
R1(config-subif)#ip address 192.168.100.1 255.255.255.0
R1(config-subif)#exit
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to
up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to
up
```

VERIFYING VLAN CONFIGURATION

```
S1#
S1#
S1#
S1#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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, Gig0/1
                                                 Gig0/2
40   Engineering_VLAN                  active    Fa0/2, Fa0/3, Fa0/4
50   Marketing_VLAN                    active    Fa0/5
60   Finance_VLAN                      active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

```
S3#
S3#
S3#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      100
Fa0/2       on           802.1q         trunking      100
Fa0/3       on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/1       40,50,60,100
Fa0/2       40,50,60,100
Fa0/3       40,50,60,100

Port        Vlans allowed and active in management domain
Fa0/1       40,50,60,100
Fa0/2       40,50,60,100
Fa0/3       40,50,60,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       40,50,60,100
Fa0/2       40,50,60,100
Fa0/3       40,50,60,100

S3#
```

6. OSPF CONFIGURATION

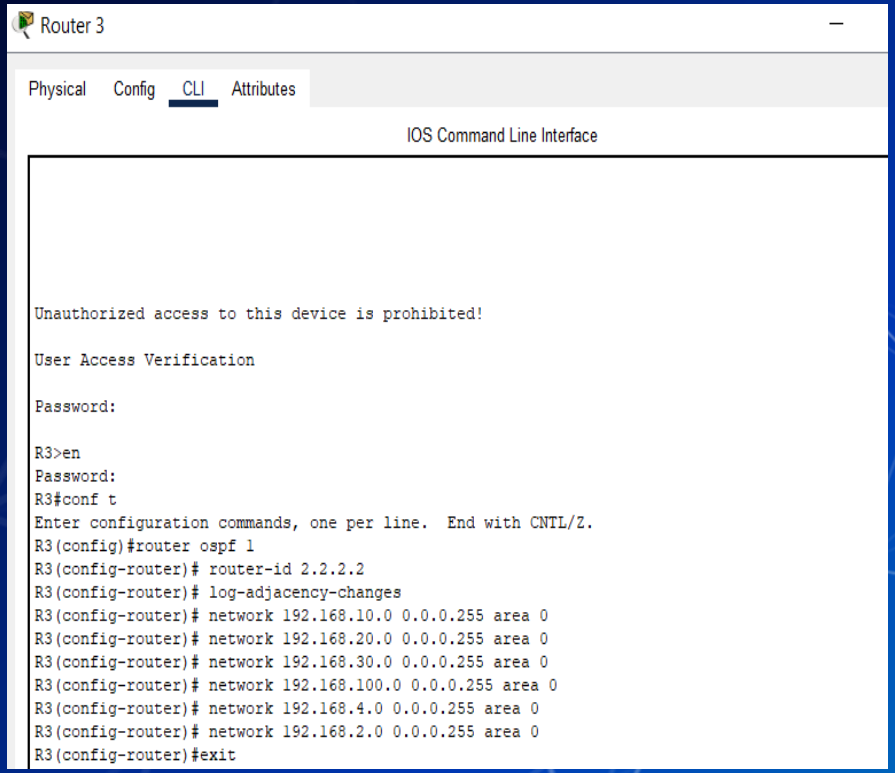
OSPF

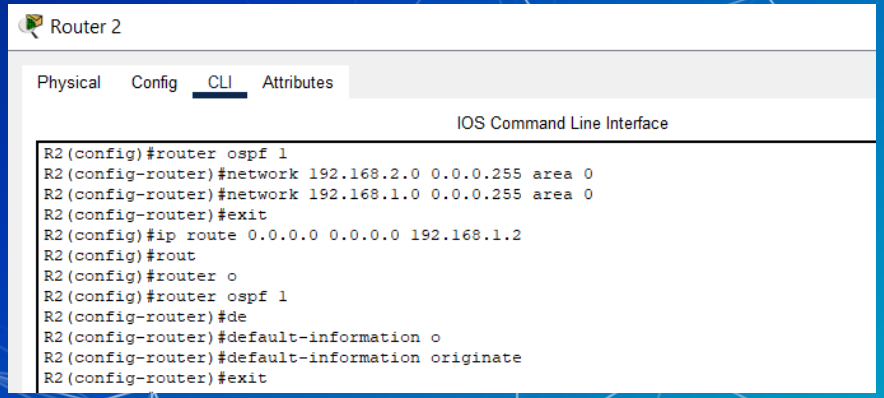
OSPF (Open Shortest Path First) is a dynamic routing protocol that efficiently finds the best path for data across networks by exchanging routing information between routers. It adapts to network changes in real-time, ensuring optimal routing.

Importance:

OSPF is crucial for large, scalable networks due to its ability to quickly converge and maintain accurate routing tables, ensuring consistent network performance.

OSPF CONFIGURATION





VERIFYING OSPF CONFIGURATION

Router 1

Physical Config CLI Attributes

IOS Command Line Interface

```
Password:

R1>en
Password:
R1#sh 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 a
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.2/32 is directly connected, GigabitEthernet0/1
O    192.168.2.0/24 [110/2] via 192.168.1.1, 01:02:49, GigabitEthernet0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
O    192.168.4.0/24 [110/3] via 192.168.1.1, 01:02:39, GigabitEthernet0/1
O    192.168.10.0/24 [110/3] via 192.168.1.1, 01:02:39, GigabitEthernet0/1
O    192.168.20.0/24 [110/3] via 192.168.1.1, 01:02:39, GigabitEthernet0/1
O    192.168.30.0/24 [110/3] via 192.168.1.1, 01:02:39, GigabitEthernet0/1
     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.40.0/24 is directly connected, GigabitEthernet0/0.40
L       192.168.40.1/32 is directly connected, GigabitEthernet0/0.40
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, GigabitEthernet0/0.50
L       192.168.50.1/32 is directly connected, GigabitEthernet0/0.50
     192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.60.0/24 is directly connected, GigabitEthernet0/0.60
L       192.168.60.1/32 is directly connected, GigabitEthernet0/0.60
     192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.100.0/24 is directly connected, GigabitEthernet0/0.100
L       192.168.100.1/32 is directly connected, GigabitEthernet0/0.100
O*E2 0.0.0.0/0 [110/1] via 192.168.1.1, 01:02:49, GigabitEthernet0/1
```

Router 2

Physical Config CLI Attributes

IOS Command Line Interface

```
R2#  sh 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 a
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/1
L       192.168.2.1/32 is directly connected, GigabitEthernet0/1
O    192.168.3.0/24 [110/2] via 192.168.1.2, 00:58:34, GigabitEthernet0/0
O    192.168.4.0/24 [110/2] via 192.168.2.2, 00:58:34, GigabitEthernet0/1
O    192.168.10.0/24 [110/2] via 192.168.2.2, 00:58:34, GigabitEthernet0/1
O    192.168.20.0/24 [110/2] via 192.168.2.2, 00:58:34, GigabitEthernet0/1
O    192.168.30.0/24 [110/2] via 192.168.2.2, 00:58:34, GigabitEthernet0/1
O    192.168.40.0/24 [110/2] via 192.168.1.2, 00:58:34, GigabitEthernet0/0
O    192.168.50.0/24 [110/2] via 192.168.1.2, 00:58:34, GigabitEthernet0/0
O    192.168.60.0/24 [110/2] via 192.168.1.2, 00:58:34, GigabitEthernet0/0
O    192.168.100.0/24 [110/2] via 192.168.1.2, 00:58:34, GigabitEthernet0/0
                      [110/2] via 192.168.2.2, 00:58:34, GigabitEthernet0/1
S*   0.0.0.0/0 [1/0] via 192.168.1.2
```

7.
ADVANCES SECURITY FEATURES

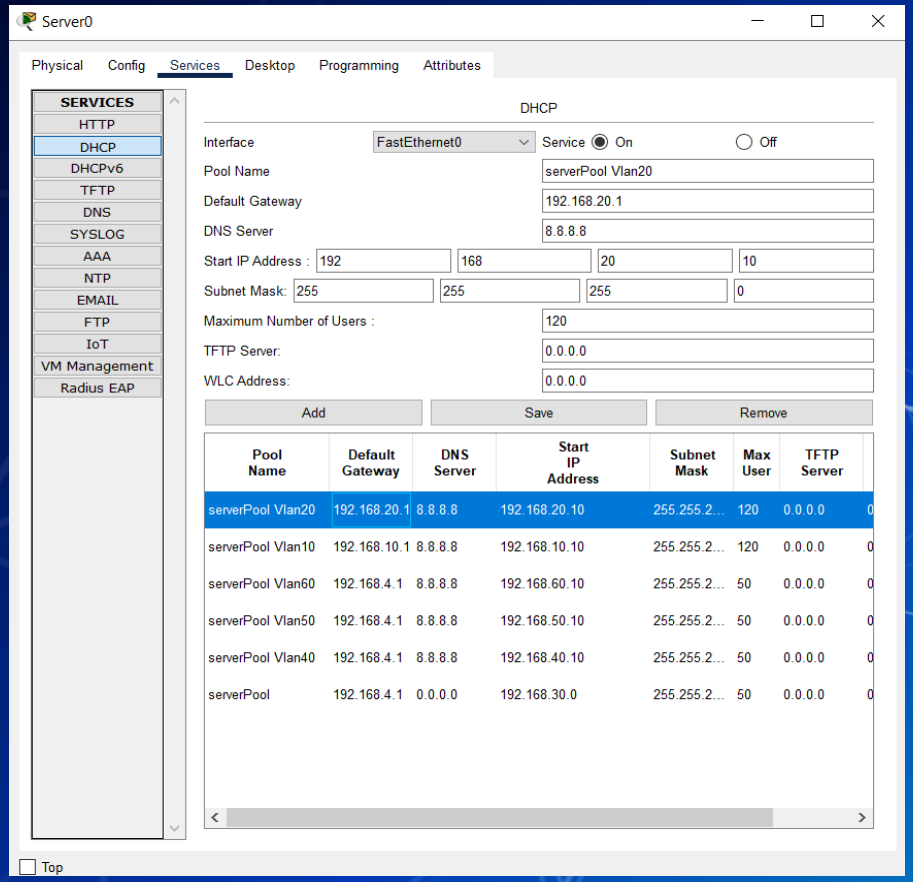
1- DHCP SNOOPING

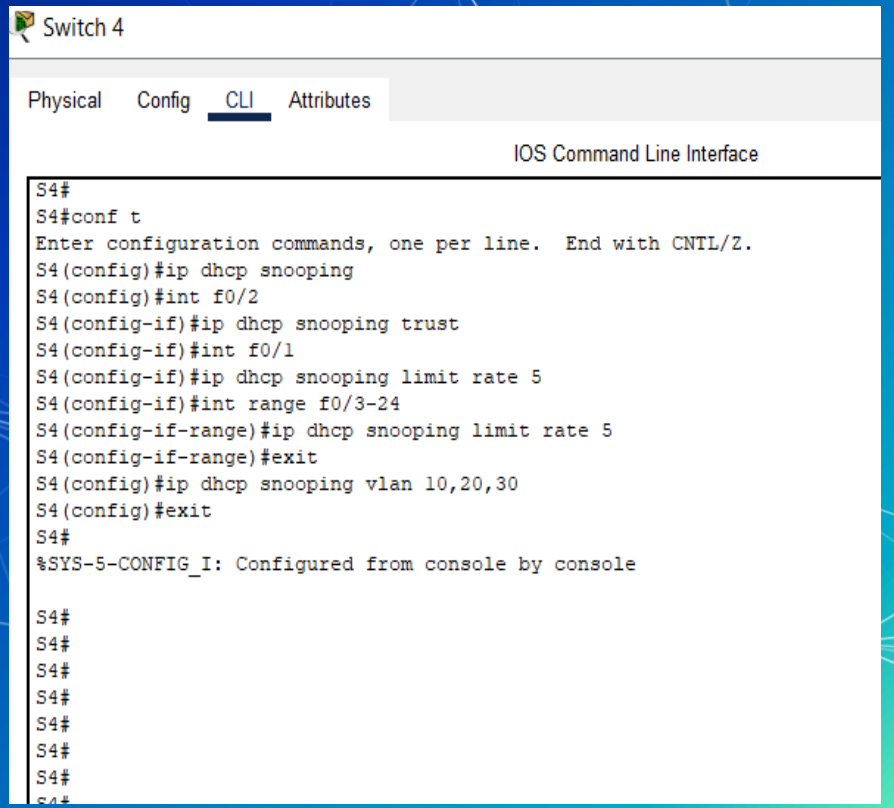
Protection Against Rogue DHCP Servers:

- DHCP Snooping is a security feature that prevents unauthorized (rogue) DHCP servers from allocating IP addresses within the network. It allows only trusted DHCP servers to provide IP configurations, filtering out any malicious DHCP offers.

- This ensures that devices receive legitimate network settings, preventing man-in-the-middle attacks.

DHCP SNOOPING CONFIGURATION





2- Dynamic ARP Inspection (DAI)

```
S4>enable
Password:
S4#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:4A:CD:CD:52   192.168.10.10    0           dhcp-snooping  10    FastEthernet0/3
00:01:C7:E5:EE:31   192.168.20.10    0           dhcp-snooping  20    FastEthernet0/4
00:30:A3:63:98:E0   192.168.20.12    0           dhcp-snooping  20    FastEthernet0/5
Total number of bindings: 3
S4#
S4#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S4(config)#ip arp inspection vlan 20
S4(config)#interface fastethernet 0/2
S4(config-if)#ip arp inspection trust
S4(config-if)#exit
S4(config)#end
```

Prevention of ARP Poisoning Attacks:

- DAI protects the network by validating ARP packets before they are forwarded. It checks the IP-to-MAC address bindings against a trusted database to ensure the authenticity of ARP requests and replies.
- By preventing malicious ARP responses, DAI thwarts ARP poisoning attacks, which could otherwise redirect traffic or intercept sensitive data.

3- IP Source Guard

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# interface gigabitEthernet 0/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# exit
Switch(config)# interface gigabitEthernet 0/2
Switch(config-if)# ip verify source
Switch(config-if)# exit
Switch# show ip verify source
Switch# show ip dhcp snooping binding
```

Restricting IP Traffic on Untrusted Layer 2 Interfaces:

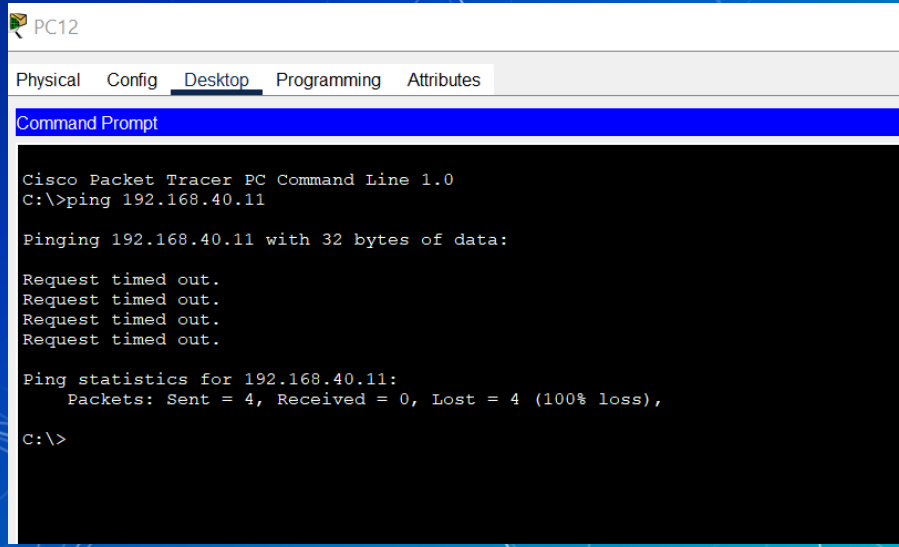
- IP Source Guard restricts IP traffic on untrusted Layer 2 interfaces by allowing only traffic from devices with matching IP and MAC address pairs.

- This ensures that only legitimate devices can communicate on the network and helps prevent IP spoofing attacks, enhancing overall network security.

8.
TSTING AND VLAIDATION

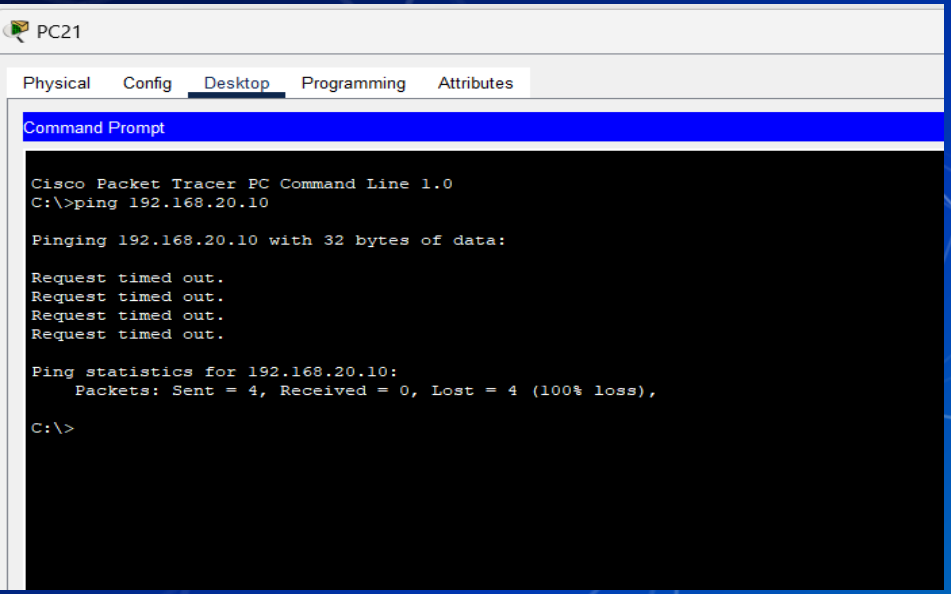
PORT SECURITY VIOLATION

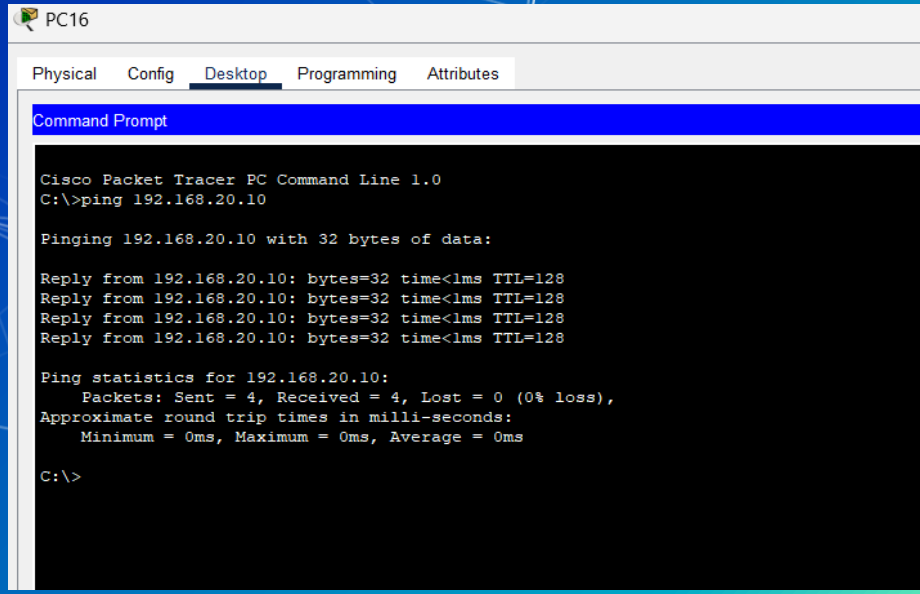
```
Press RETURN to get started!

Unauthorized access to this device is prohibited!

User Access Verification

Password:
Password:

S1>en
Password:
S1#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0000.0C20.5BEA:40
Security Violation Count   : 0

S1#
```



DYNAMIC ARP INSPECTION

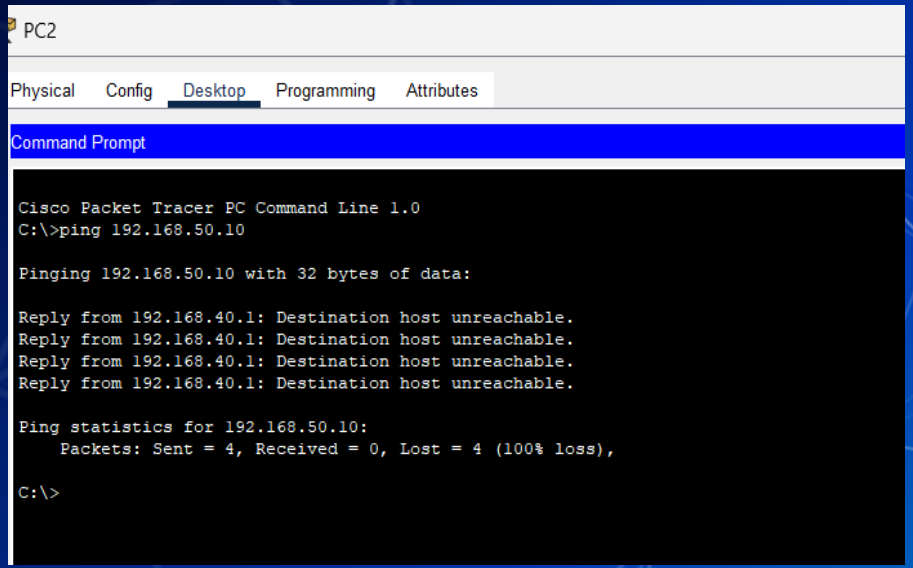
PC21 cannot ping PC20 despite it have an IP address in the same range of VLAN 20 Because they are not in the same VLAN



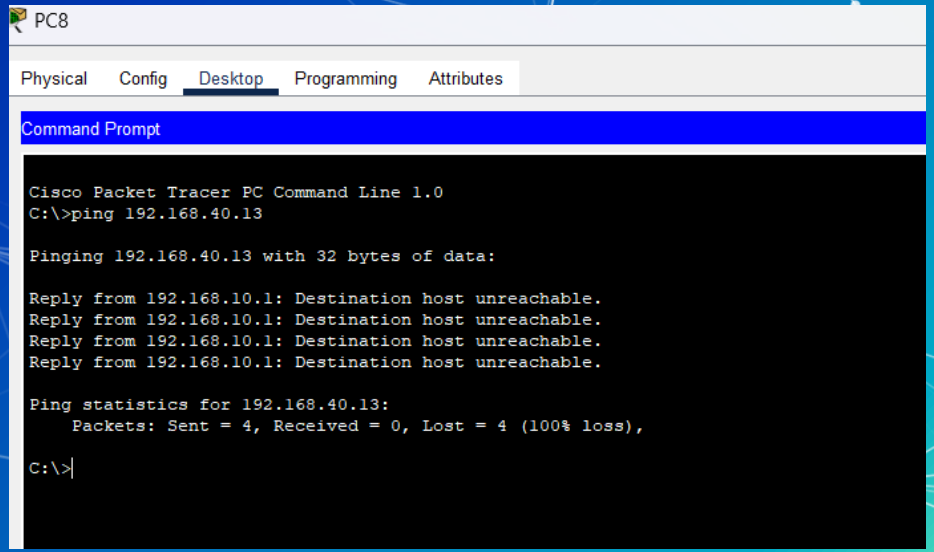


STANDARD ACL

BLOCK_VLAN 40_VLAN 50

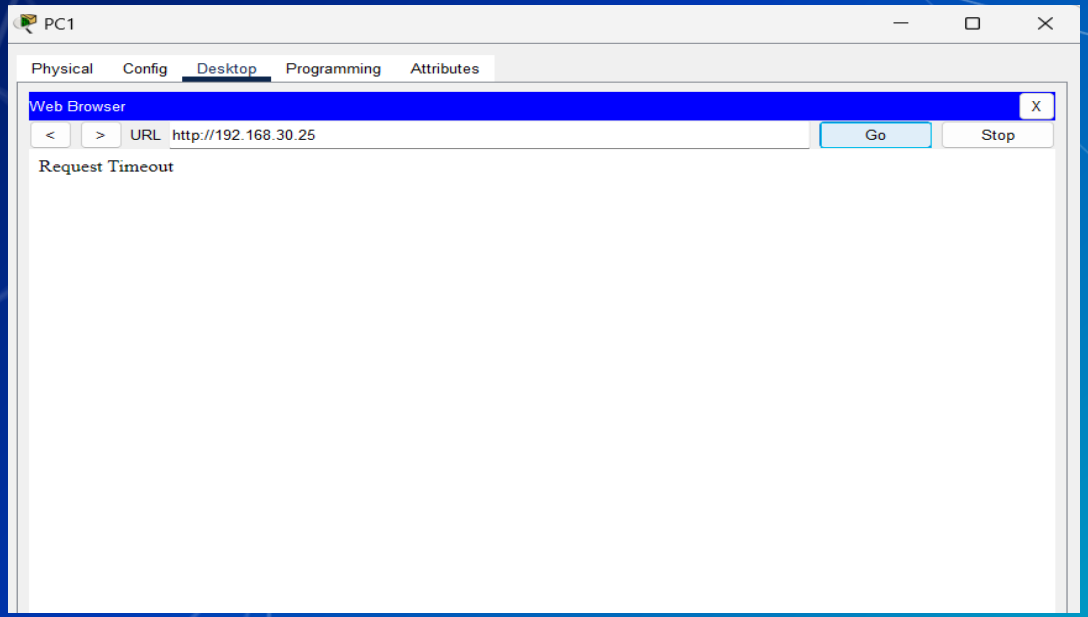


STANDARD ACLs PC 8



EXTENDED ACL

PC1 Extended ACLs TCP



9. CONCLUSION AND RECOMMENDATIONS

Conclusion and Recommendations

Conclusion:

This project has implemented essential security measures, including Access Control Lists (ACLs) for traffic management, DHCP Snooping to thwart rogue DHCP servers, Dynamic ARP Inspection (DAI) to prevent ARP poisoning, and IP Source Guard to limit unauthorized IP traffic. These measures significantly enhance the security posture of the network by isolating critical resources, preventing unauthorized access, and ensuring the integrity of data communications.

Recommendations:

- Firewalls: Introduce firewalls to add an extra layer of protection against external threats and manage traffic flow effectively.
- Intrusion Detection/Prevention Systems (IDS/IPS): Implement IDS/IPS to monitor network traffic for anomalies and take proactive measures against potential threats.
- Regular Security Audits: Conduct routine security audits to identify vulnerabilities and ensure that security protocols remain effective and current.

10. Q&A


THANKS!