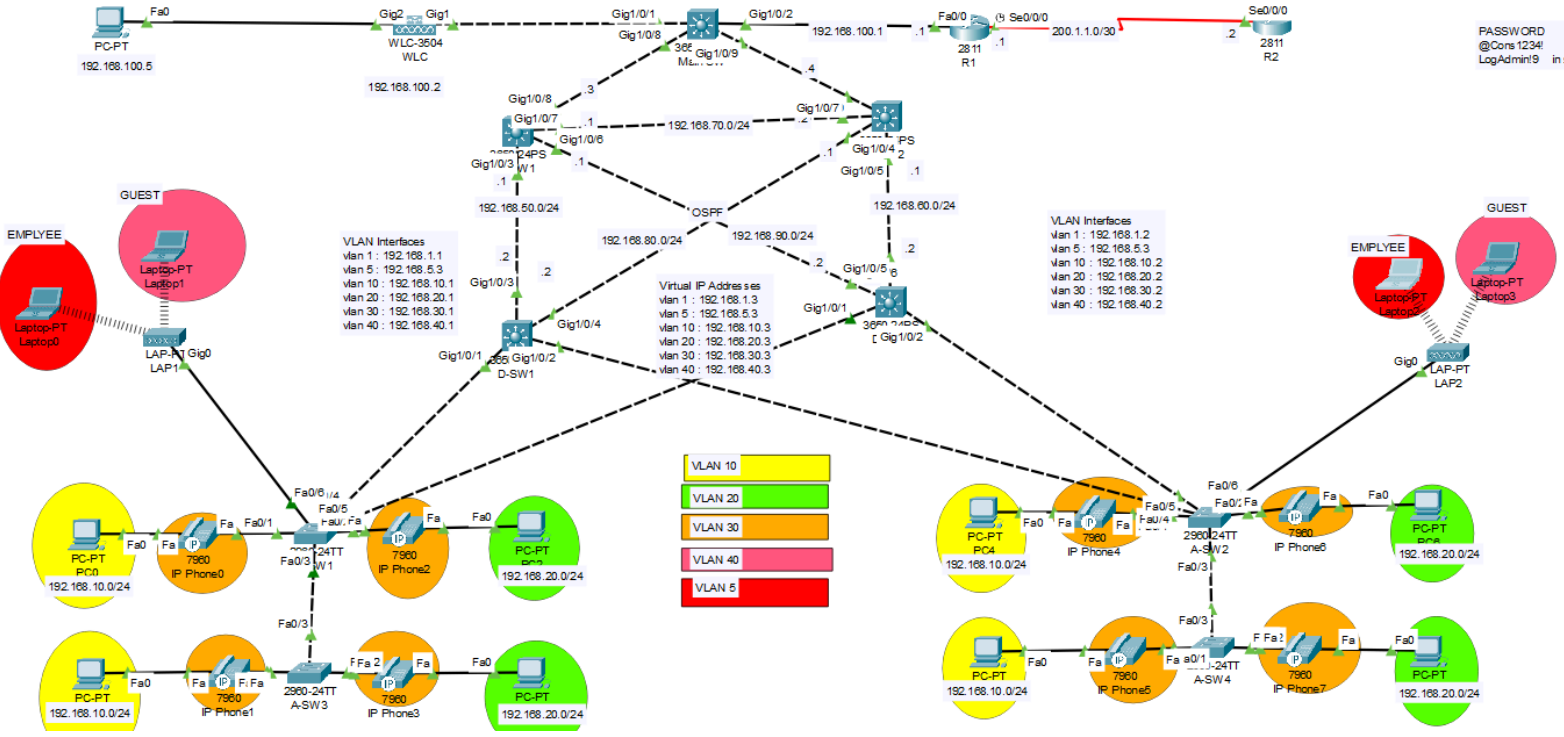
Egypt Digital Pioneers Initiative (EDPI)

Final Project

Comprehensive Network Infrastructure Setup

Network Topology Diagram



This project aims to design and implement a scalable, secure, and efficient network infrastructure for the organization. The solution integrates advanced technologies to ensure optimal performance, strong security, and adaptability to future needs.

Technologies Used

1. VLANs for Network Segmentation
2. High Availability with HSRP
3. Dynamic Routing with OSPF
4. DHCP (Dynamic Host Configuration Protocol)
5. IP Telephony with QoS (Quality of Service)
6. Wireless LAN with Security
7. Access Control Lists (ACLs)
8. Port Address Translation (PAT)
9. SSH (Secure Shell) for Remote Access
10. LAN Security Measures:
    - Port Security
    - BPDU Guard (Spanning Tree Protocol Protection)
    - Root Guard
    - DHCP Snooping
    - Dynamic ARP Inspection (DAI)
    - Storm Control
    - VLAN Hopping Prevention

■ Key Components:

1-VLANs for Network Segmentation:

- VLANs (Virtual Local Area Networks) were configured to segment the network into distinct logical groups. Each VLAN isolates traffic and enhances network security.

    - VLAN 1 : Native (192.168.10.0/24)
    - VLAN 10: Guest Network (192.168.10.0/24)
    - VLAN 20: Network 20 (192.168.10.0/24)
    - VLAN 5: Employee Network (192.168.5.0/24)
    - VLAN 30: VoIP (Voice over IP) (192.168.30.0/24)
    - VLAN 40: GUEST Network (192.168.40.0/24)

■ A-SW1

```
enable
conf t
vlan 10
exit
vlan 20
exit
vlan 30
exit
vlan 40
name Guest
vlan 5
name Employee
end
interface range F0/3-6
switchport mode trunk
interface fa0/1
sw mode access
switchport access vlaN 10
switchport voice vlan 30
interface fa0/2
sw mode access
switchport access vlan 20
switchport voice vlan 30
end
```

■ A-SW2

```
enable
conf t
vlan 10
exit
vlan 20
exit
vlan 30
exit
vlan 40
name Guest
vlan 5
name Employee
end
interface range F0/3-6
switchport mode trunk
interface fa0/1
sw mode access
switchport access vlaN 10
switchport voice vlan 30
interface fa0/2
sw mode access
switchport access vlan 20
switchport voice vlan 30
end
```

2-High Availability with HSRP:

- HSRP (Hot Standby Router Protocol) was configured for router redundancy. This ensures that if the active router fails, a backup router automatically takes over, minimizing downtime.

D-SW1 standby

```
enable
conf t
vlan 10
exit
vlan 20
exit
vlan 30
exit
vlan 40
name Guest
vlan 5
name Employee
end
ip routing
interface range gig1/0/1 - 2
switchport mode trunk
end
```

```
iinterface vlan 1
standby 1 ip 192.168.1.3
standby 1 priority 101
standby 1 preempt
interface vlan 10
standby 10 ip 192.168.10.3
standby 10 priority 101
standby 10 preempt
interface vlan 20
standby 20 ip 192.168.20.3
standby 20 priority 101
standby 20 preempt
interface vlan 30
standby 30 ip 192.168.30.3
standby 30 priority 101
standby 30 preempt
interface vlan 40
standby 40 ip 192.168.40.3
standby 40 priority 101
standby 40 preempt
interface vlan 5
standby 5 ip 192.168.5.3
standby 5 priority 101
standby 5 preempt
 end
```

D-SW2 Backup

```
enable
conf t
vlan 10
exit
vlan 20
exit
vlan 30
exit
vlan 40
name Guest
vlan 5
name Employee
end
ip routing
iinterface range gig1/0/1 - 2
switchport mode trunk
end
conf t
interface vlan 1
standby 1 ip 192.168.1.3
interface vlan 10
standby 10 ip 192.168.10.3
interface vlan 20
standby 20 ip 192.168.20.3
interface vlan 30
standby 30 ip 192.168.30.3
interface vlan 40
standby 40 ip 192.168.40.3
interface vlan 5
standby 5 ip 192.168.5.3
 end
```

3-Dynamic Routing with OSPF:

- OSPF (Open Shortest Path First) was implemented for dynamic routing between different networks. It ensures optimal path selection for data transmission.
- All switches and routers exchange routing information dynamically, improving network scalability and redundancy.

D-SW1 standby

```
ip routing
int Gig1/0/3
no switchport
ip add 192.168.50.2 255.255.255.0
no sh
exit
int Gig1/0/4
no switchport
ip add 192.168.80.2 255.255.255.0
no sh
exit
router ospf 1
router-id 1.1.1.1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.80.0 0.0.0.255 area 0
exit
```

D-SW2 Backup

```
ip routing
int Gig1/0/3
no switchport
ip add 192.168.60.2 255.255.255.0
no sh
exit
int Gig1/0/4
no switchport
ip add 192.168.90.2 255.255.255.0
no sh
exit
router ospf 1
router-id 2.2.2.2
network 192.168.1.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
network 192.168.90.0 0.0.0.255 area 0
exit
```

C-SW1

```
en
conf t
hostname C-SW1
ip routing
int Gig1/0/1
no switchport
ip add 192.168.95.3 255.255.255.0
no sh
exit
int Gig1/0/5
no switchport
ip add 192.168.70.3 255.255.255.0
no sh
exit
int Gig1/0/3
no switchport
ip add 192.168.50.3 255.255.255.0
no sh
exit
int Gig1/0/4
no switchport
ip add 192.168.90.3 255.255.255.0
no sh
exit
router ospf 1
router-id 3.3.3.3
network 192.168.50.0 0.0.0.255 area 0
network 192.168.90.0 0.0.0.255 area 0
network 192.168.95.0 0.0.0.255 area 0
network 192.168.70.0 0.0.0.255 area 0
exit
```

C-SW2

```
en
conf t
hostname C-SW2
ip routing
int Gig1/0/2
no switchport
ip add 192.168.99.3 255.255.255.0
no sh
exit
int Gig1/0/3
no switchport
ip add 192.168.60.3 255.255.255.0
no sh
exit
int Gig1/0/4
no switchport
ip add 192.168.80.3 255.255.255.0
no sh
exit
int Gig1/0/5
no switchport
ip add 192.168.70.2 255.255.255.0
no sh
exit
router ospf 1
router-id 4.4.4.4
network 192.168.99.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
network 192.168.70.0 0.0.0.255 area 0
network 192.168.80.0 0.0.0.255 area 0
exit
```

core-SW

```
econf t
interface range gig1/0/4-
5,gig1/0/7,gig1/0/9
no switchport
end
ienable
conf t
interface range gig1/0/3,gig1/0/6-8
no switchport
end
conf t
interface range gig1/0/6
no switchport
end
interface gig1/0/5
ip add 192.168.60.2 255.255.255.0
interface gig1/0/6
ip add 192.168.90.2 255.255.255.0
end
int Gig1/0/4
no switchport
ip add 192.168.110.2 255.255.255.0
no sh
exit
ip routing
router ospf 1
router-id 1.1.1.1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.80.0 0.0.0.255 area 0
end
```

Router1

```
en
conf t
hostname R0
int fa0/0
ip add 192.168.110.1 255.255.255.0
no sh
exit
int Se0/1/0
ip add 200.1.1.1 255.255.255.0
no sh
exit
router ospf 1
router-id 6.6.6.6
network 192.168.110.0 0.0.0.255 area 0
network 200.1.1.0 0.0.0.255 area 0
exit
```

Router1

```
en
conf t
hostname R1
int Se0/1/0
ip add 200.1.1.2 255.255.255.0
no sh
exit
router ospf 1
router-id 7.7.7.7
network 200.1.1.0 0.0.0.255 area 0
exit
```

4-DHCP (Dynamic Host Configuration Protocol):

- DHCP servers were configured for automatic IP allocation to devices, making IP management easy and reducing manual configuration errors.

Router1

```
enable
conf t
ip dhcp excluded-address 192.168.40.1
192.168.40.10
ip dhcp excluded-address 192.168.30.1
192.168.30.10
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.20.1
192.168.20.10
ip dhcp excluded-address 192.168.10.1
192.168.10.10
ip dhcp excluded-address 192.168.5.1 192.168.5.10
ip dhcp pool Guest
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.3
ip dhcp pool VOIP
 network 192.168.30.0 255.255.255.0
 option 150 ip 192.168.100.1
ip dhcp pool native
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.3
 option 43 ip 192.168.100.2
ip dhcp pool vlan10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.3
ip dhcp pool vlan20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.3
 ip dhcp pool Employee
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.3
end
```

D-SW1 standby

```
inenable
conf t
interface vlan 1
ip helper-address 192.168.100.1
interface vlan 10
ip helper-address 192.168.100.1
interface vlan 20
ip helper-address 192.168.100.1
interface vlan 30
ip helper-address 192.168.100.1
interface vlan 40
ip helper-address 192.168.100.1
interface vlan 5
ip helper-address 192.168.100.1
end
```

D-SW2 Backup

```
enable
conf t
interface vlan 1
ip helper-address 192.168.100.1
interface vlan 10
ip helper-address 192.168.100.1
interface vlan 20
ip helper-address 192.168.100.1
interface vlan 30
ip helper-address 192.168.100.1
interface vlan 40
ip helper-address 192.168.100.1
interface vlan 5
ip helper-address 192.168.100.1
end
```

5-IP Telephony with QoS (Quality of Service):

- IP telephony was integrated into the network, allowing for voice communication over IP.
- QoS was configured to prioritize voice traffic, ensuring low latency for VoIP calls (VLAN 30 is dedicated to IP phones).

Router1

```
ienable
conf t
telephony-service
max-ephones 8
max-dn 8
ip source-address 192.168.100.1 port 2000
auto assign 1 to 8
exit
ephone-dn 1
number 1001
exit
ephone-dn 2
number 1002
exit
ephone-dn 3
number 1003
exit
ephone-dn 4
number 1004
exit

ephone-dn 5
number 1005
exit
ephone-dn 6
number 1006
exit
ephone-dn 7
number 1007
exit
ephone-dn 8
number 1008
end
```

6-Access Control Lists (ACLs):

- ACLs control traffic flow and ensure that only authorized devices can access specific network parts.
- Standard and extended ACLs are applied to filter traffic based on IP addresses, protocols, and ports.

7-Port Address Translation (PAT):

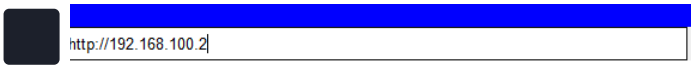
- PAT was set up for efficient internet access, allowing multiple devices within the LAN to access the internet using a single public IP address.

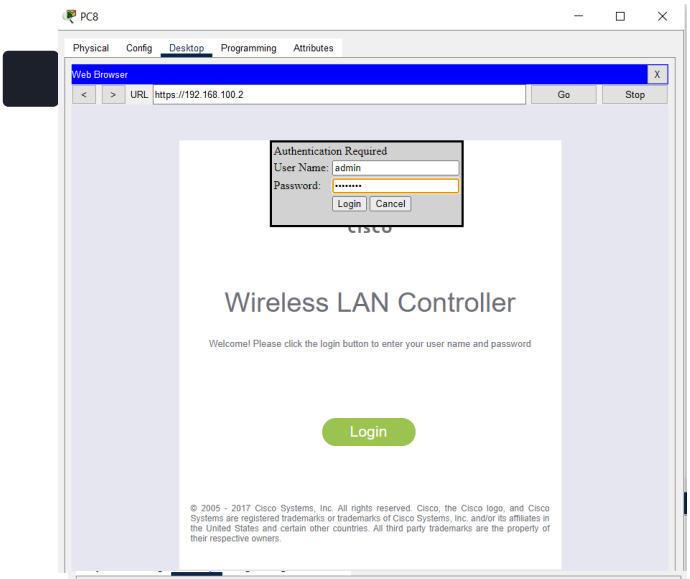
Router0

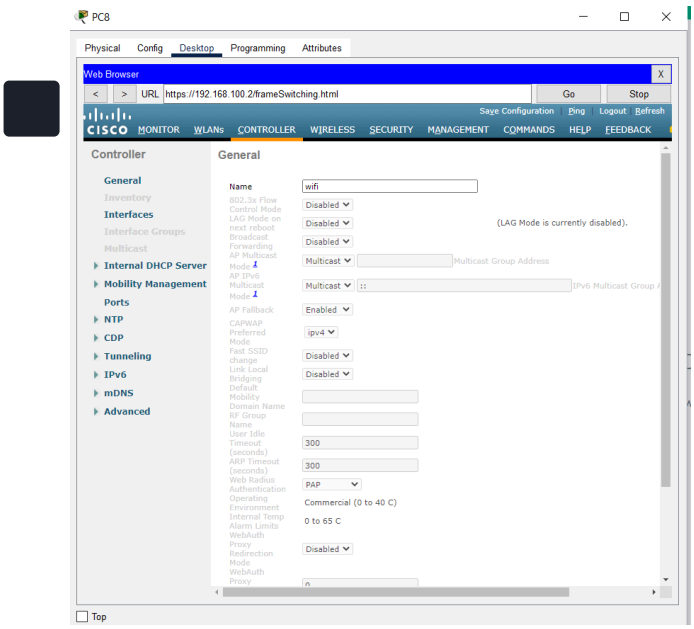
```
int fa0/0
ip nat inside

int se0/1/0
ip nat outside

access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 192.168.5.0 0.0.0.255

ip nat inside source list 1 interface fastethernet 0/1 overload
```

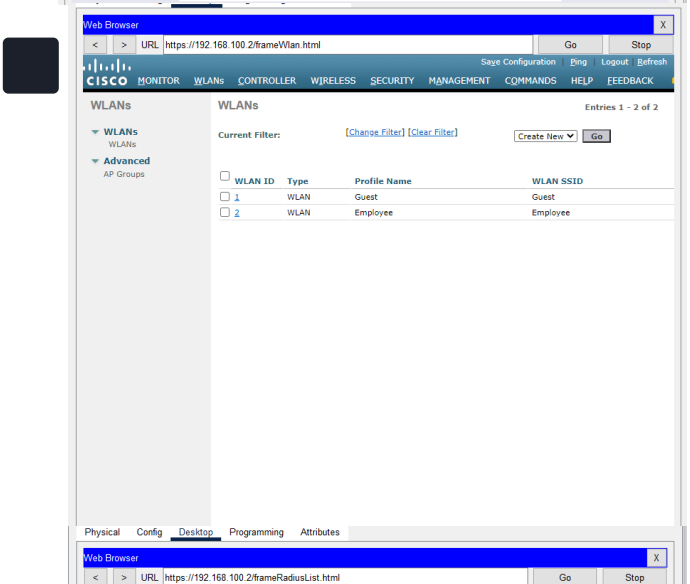
8-Wireless LAN with Security:

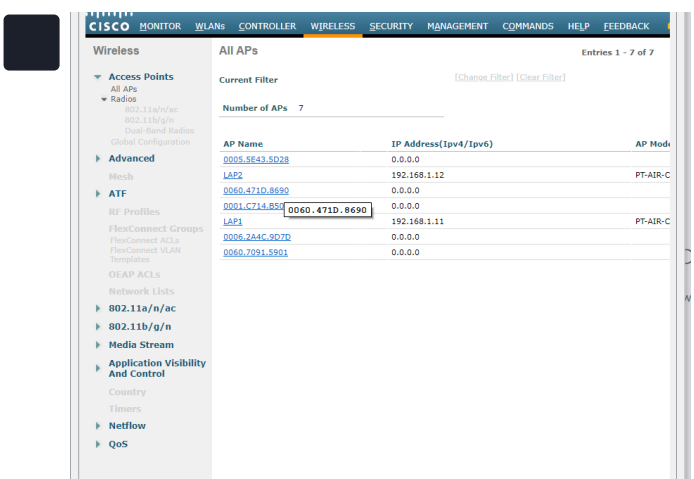
- A secure Wireless LAN (WLAN) was set up using WPA2/WPA3 encryption for secure communication.
- A Wireless LAN Controller (WLC) manages the access points, ensuring central management and security.
- Clients can connect to the wireless network securely with encrypted sessions.

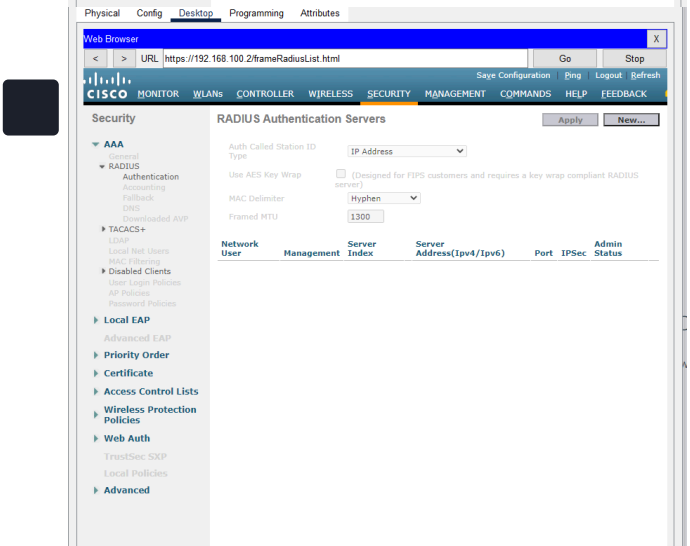












9-SSH (Secure Shell) for Remote Access:

- SSH was implemented to provide encrypted remote management of network devices, enhancing security and ensuring safe remote configuration.

in all devices

```
EN
CONF T
ip domain-name security.com
enable secret @Cons1234!
 line console 0
 password @Cons1234!
 Line vty 0 15
 username NETadmin secret
LogAdmin!9
 LINE VTY 0 15
 transport input ssh
 login local
 crypto key generate rsa
```

PC

```
ssh -l admin 192.168.40.4

pass=@Cons1234!
      =LogAdmin!9
```

A-SW1

```
interface vlan 1
ip add 192.168.1.2 255.255.255.0
no shutdown
interface vlan 10
ip add 192.168.10.2 255.255.255.0
interface vlan 20
ip add 192.168.20.2 255.255.255.0
nterface vlan 5
ip add 192.168.5.2 255.255.255.0
interface vlan 30
ip add 192.168.30.2 255.255.255.0
interface vlan 40
ip add 192.168.40.2 255.255.255.0
```

A-SW2

```
interface vlan 1
ip add 192.168.1.5 255.255.255.0
no shutdown
interface vlan 10
ip add 192.168.10.5 255.255.255.0
nterface vlan 5
ip add 192.168.5.5 255.255.255.0
interface vlan 20
ip add 192.168.20.5 255.255.255.0
interface vlan 30
ip add 192.168.30.5 255.255.255.0
interface vlan 40
ip add 192.168.40.5 255.255.255.0
```

10-LAN Security Measures:

1-Port Security:

- Port security was enabled to prevent unauthorized devices from connecting to the network.
- This feature limits the number of MAC addresses per port, protecting against MAC flooding attacks.
- Configure Violation Action (What happens when the rule is violated):
  - Protect – Only blocks traffic from violating devices.
  - Restrict – Blocks traffic and logs the violation.
  - Shutdown – Shuts down the port when a violation occurs.

A-SW1

```
En
Conf t
Int range f0/1-2
Sw mode access
Sw port-security
Int range f0/1-2
sw port-security maximum 2
Int range f0/1-2
sw port-security mac-address sticky
Int range f0/1-2
sw port-security violation restrict
```

A-SW1

```
En
Conf t
Int range f0/1-2
Sw mode access
Sw port-security
Int range f0/1-2
sw port-security maximum 2
Int range f0/1-2
sw port-security mac-address sticky
Int range f0/1-2
sw port-security violation restrict
```

2-BPDU Guard (Spanning Tree Protocol Protection):

- BPDU Guard was configured to protect the Spanning Tree Protocol (STP) from being manipulated by unauthorized devices, preventing topology changes.

D-SW1

```
enable
conf t
spanning-tree vlan 1 root primary
spanning-tree vlan 10 root primary
spanning-tree vlan 20 root primary
spanning-tree vlan 30 root primary
spanning-tree vlan 40 root primary
spanning-tree vlan 5 root primary
```

D-SW2

```
enable
conf t
spanning-tree vlan 1 root secondary
spanning-tree vlan 10 root secondary
spanning-tree vlan 20 root secondary
spanning-tree vlan 30 root secondary
spanning-tree vlan 40 root secondary
spanning-tree vlan 5 root primary
end
```

3-Root Guard:

- Used Root Guard to prevent devices from attempting to become the root bridge in the spanning tree.

A-SW1

```
int fa0/1
spanning-tree guard root
```

A-SW2

```
int fa0/1
spanning-tree guard root
```

4-Segmentation, Targeting, Positioning (STP):

- A marketing model that helps businesses identify their target market and position their products effectively. • Segmentation involves dividing the market into distinct groups based on characteristics like demographics, psychographics, or behavior.

A-SW1

en
conf t
int range f0/1-2
spanning-tree portfast
int range f0/1-2
spanning-tree bpduguard enable

A-SW1

en
conf t
int range f0/1-2
spanning-tree portfast
int range f0/1-2
spanning-tree bpduguard enable

7-VLAN Hopping Prevention:

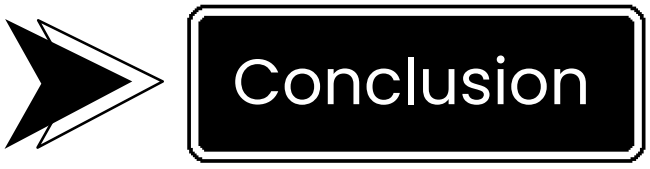
- VLAN Hopping Prevention was enabled to prevent attacks where a device tries to send traffic across VLANs it is not authorized to access.

A-SW1

int fa0/1
switchport nonegotiate

A-SW12

int fa0/1
switchport nonegotiate



This network infrastructure setup provides a highly scalable, secure, and efficient solution tailored to the organization's needs. It combines advanced routing, IP telephony with QoS, secure wireless communication, and robust security measures to protect the integrity and availability of the network.

Thank You!

designed by

Mazen Farg

Let's Get In Touch

Linkedin Mazen _Farg

E-mail mazenf948@gmail.com

01554956890