



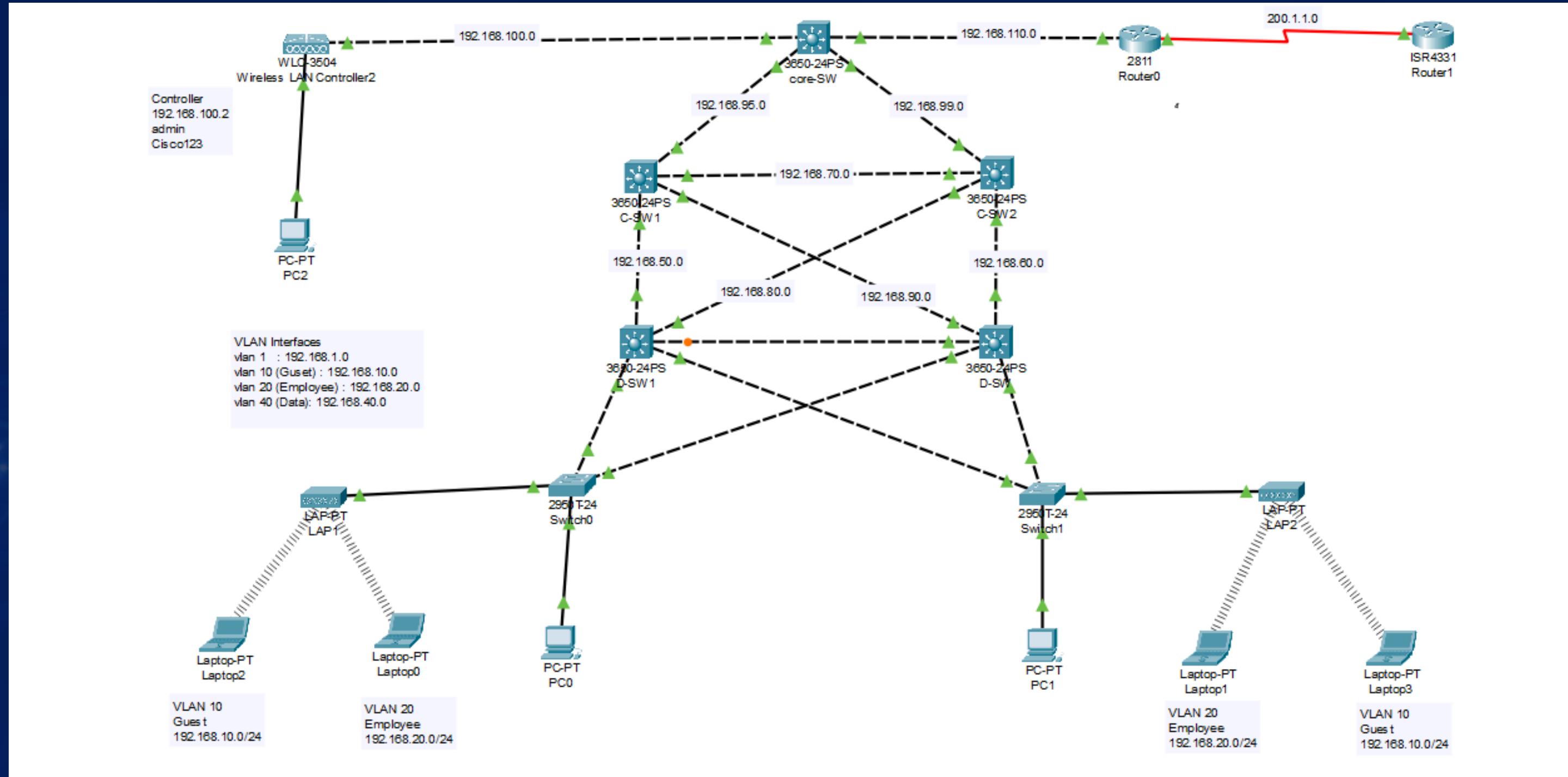
Thynk Unlimited



# COMPREHENSIVE NETWORK INFRASTRUCTURE SETUP

Under Supervision of : DR/Hassan Shaban

# TOPOLOGY





## VLANs for Network Segmentation:

### A-SW1

```
en
conf t
hostname A-SW1
  vlan 1
  vlan 10
  name GUST
  vlan 20
  name EMPLOYEE
  vlan 30
  name VOIP
  vlan 40
  name DATA
  exit
  int fa0/1
sw mode access
sw access vlan 40
sw voice vlan 30
  exit
  int fa0/2
sw mode trunk
  exit
int rang Gig0/1-2
sw mode trunk
  exit
```

### A-SW2

```
en
conf t
hostname A-SW2
  vlan 1
  vlan 10
  name GUST
  vlan 20
  name EMPLOYEE
  vlan 30
  name VOIP
  vlan 40
  name DATA
  exit
  int fa0/1
sw mode access
sw access vlan 40
sw voice vlan 30
  exit
  int fa0/2
sw mode trunk
  exit
int rang Gig0/1-2
sw mode trunk
  exit
```

VLAN 1: Native (192.168.10.0/24)

VLAN 10: Guest Network (192.168.10.0/24)

VLAN 20: Employee Network (192.168.20.0/24)

VLAN 40: Data Network (192.168.40.0/24)

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



## ■ High Availability with HSRP:

### ■ D-SW1 standby

```
en
conf t
hostname D-SW1
  vlan 1
  vlan 10
  name GUST
  vlan 20
  name EMPLOYEE
    vlan 30
    name VOIP
    vlan 40
    name DATA
      exit
    ip routing
    int Gig1/0/1
    sw mode trunk
      exit
    int Gig1/0/2
    sw mode trunk
      exit
    int vlan 1
    ip add 192.168.1.1 255.255.255.0
      standby version 2
      standby 5 ip 192.168.1.3
      standby 5 priority 150
      standby 5 preempt
      no sh
      exit
```

```
int vlan 10
ip add 192.168.10.1 255.255.255.0
  standby version 2
  standby 1 ip 192.168.10.3
  standby 1 priority 150
  standby 1 preempt
  no sh
  exit
int vlan 20
ip add 192.168.20.1 255.255.255.0
  standby version 2
  standby 2 ip 192.168.20.3
  standby 2 priority 150
  standby 2 preempt
  no sh
  exit
int vlan 30
ip add 192.168.30.1 255.255.255.0
  standby version 2
  standby 3 ip 192.168.30.3
  standby 3 priority 150
  standby 3 preempt
  no sh
  exit
int vlan 40
ip add 192.168.40.1 255.255.255.0
  standby version 2
  standby 4 ip 192.168.40.3
  standby 4 priority 150
  standby 4 preempt
  no sh
  exit
```

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





## ■ High Availability with HSRP:

### ■ D-SW2 Backup

```
en
conf t
hostname D-SW2
  vlan 1
  vlan 10
    name GUST
  vlan 20
    name EMPLOYEE
    vlan 30
    name VOIP
    vlan 40
    name DATA
      exit
    ip routing
    int Gig1/0/1
    sw mode trunk
      exit
    int Gig1/0/2
    sw mode trunk
      exit
    int vlan 1
    ip add 192.168.1.2 255.255.255.0
      standby version 2
      standby 1 ip 192.168.1.3
        no sh
        exit
```

```
int vlan 10
ip add 192.168.10.2 255.255.255.0
  standby version 2
  standby 1 ip 192.168.10.3
    no sh
    exit
  int vlan 20
  ip add 192.168.20.2 255.255.255.0
    standby version 2
    standby 2 ip 192.168.20.3
      no sh
      exit
    int vlan 30
    ip add 192.168.30.2 255.255.255.0
      standby version 2
      standby 3 ip 192.168.30.3
        no sh
        exit
      int vlan 40
      ip add 192.168.40.2 255.255.255.0
        standby version 2
        standby 4 ip 192.168.40.3
          no sh
          exit
```

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





## ■ Dynamic Routing with OSPF:

### ■ 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 192.168.40.0 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 192.168.40.0 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
```

- 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.





## ■ Dynamic Routing with OSPF:

### ■ 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

```
en  
conf t  
hostname core-SW1  
ip routing  
int Gig1/0/1  
no switchport  
ip add 192.168.95.2 255.255.255.0  
no sh  
exit  
int Gig1/0/2  
no switchport  
ip add 192.168.99.2 255.255.255.0  
no sh  
exit  
int Gig1/0/3  
no switchport  
ip add 192.168.100.1 255.255.255.0  
no sh  
exit  
int Gig1/0/4  
no switchport  
ip add 192.168.110.2 255.255.255.0  
no sh  
exit  
router ospf 1  
router-id 5.5.5.5  
network 192.168.95.0 0.0.0.255 area 0  
network 192.168.99.0 0.0.0.255 area 0  
network 192.168.100.0 0.0.0.255 area 0  
network 192.168.110.0 0.0.0.255 area 0  
exit
```

### ■ Router0

```
en  
conf t  
hostname R0  
int fa0/0  
ip add 192.168.110.1 255.255.255.255.0  
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
```



## ■ DHCP (Dynamic Host Configuration Protocol):

### ■ Router0

```
ip dhcp excluded-address 192.168.1.1
    192.168.1.10
ip dhcp excluded-address 192.168.10.1
    192.168.10.10
ip dhcp excluded-address
    192.168.20.1 192.168.20.10
ip dhcp excluded-address
    192.168.30.1 192.168.30.10
ip dhcp excluded-address
    192.168.40.1 192.168.40.10
    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 Guest
network 192.168.10.0 255.255.255.0
    default-router 192.168.10.3
    ip dhcp pool Employee
network 192.168.20.0 255.255.255.0
    default-router 192.168.20.3
    ip dhcp pool Voice
network 192.168.30.0 255.255.255.0
    default-router 192.168.30.3
    option 150 ip 192.168.110.1
        ip dhcp pool Data
network 192.168.40.0 255.255.255.0
    default-router 192.168.40.3
```

### ■ D-SW1 standby

```
interface vlan 1
ip helper-address 192.168.110.1
    interface vlan 10
ip helper-address 192.168.110.1
    interface vlan 20
ip helper-address 192.168.110.1
    interface vlan 30
ip helper-address 192.168.110.1
    interface vlan 40
ip helper-address 192.168.110.1
```

### ■ D-SW1 standby

```
interface vlan 1
ip helper-address 192.168.110.1
    interface vlan 10
ip helper-address 192.168.110.1
    interface vlan 20
ip helper-address 192.168.110.1
    interface vlan 30
ip helper-address 192.168.110.1
    interface vlan 40
ip helper-address 192.168.110.1
```

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



## ■ Access Control Lists (ACLs) & Port Address Translation (PAT):

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

- 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.

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





## Wireless LAN with Security:

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

**Monitor**

**Summary**

150 Access Points Supported

Cisco 3500 Series Wireless Controller  
Model 3504

**Controller Summary**

Management IP Address	192.168.100.2 , ::/128
Software Version	8.3.111.0
Field Recovery Image Version	7.6.101.1
System Name	WLC
Up Time	3 hours, 18 minutes, 43 seconds
System Time	Sat Oct 12 20:44:26 2024
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/0%
Memory Usage	46%
Fan Status	3800 rpm

**Rogue Summary**

Active Rogue APs	0	<a href="#">Detail</a>
Active Rogue Clients	0	<a href="#">Detail</a>
Adhoc Rogues	0	<a href="#">Detail</a>
Rogues on Wired Network	0	

**Top WLANs**

Profile Name	# of Clients

**Most Recent Traps**

[View All](#)

**Top Applications**

Application Name	Packet Count	Byte Count

[View All](#)

- 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.





## ■ SSH (Secure Shell) for Remote Access:

### ■ in all devices

```
ip domain-name security.com
crypto key generate rsa
    1024
username admin privilege 15 secret
    cisco123
line vty 0 4
    login local
    transport input ssh
    ip ssh version 2
    exec-timeout 5 0
```

### ■ A-SW1

```
interface vlan 1
ip add 192.168.1.4 255.255.255.0
    no shutdown
interface vlan 10
ip add 192.168.10.4 255.255.255.0
    interface vlan 20
ip add 192.168.20.4 255.255.255.0
    interface vlan 30
ip add 192.168.30.4 255.255.255.0
    interface vlan 40
ip add 192.168.40.4 255.255.255.0
```

03

### ■ A-SW1

```
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
    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
```

### ■ PC

```
ssh -l admin 192.168.40.4
pass=cisco123
```

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





## ■ Port Security:

### ■ A-SW1

```
int fa0/1
sw mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address
sticky
switchport port-security violation restrict
```

### ■ A-SW2

```
int fa0/1
sw mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
```

- 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 rules violated):
  - Protect – Only blocks traffic from violating devices.
  - Restrict – Blocks traffic and logs the violation.
  - Shutdown – Shuts down the port when a violation occurs.



## ■ BPDU Guard (Spanning Tree Protocol Protection):

### ■ A-SW1

```
spanning-tree portfast bpduguard default
    int fa0/1
spanning-tree portfast
```

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

### ■ A-SW2

```
spanning-tree portfast bpduguard default
    int fa0/1
spanning-tree portfast
```

## ■ Root Guard:

### ■ A-SW1

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

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

### ■ A-SW2

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





## ■ DHCP Snooping:

### ■ A-SW1

```
ip dhcp snooping
ip dhcp snooping vlan 1
ip dhcp snooping vlan 10
ip dhcp snooping vlan 20
ip dhcp snooping vlan 30
ip dhcp snooping vlan 40
    int range gig 0/1-2
    ip dhcp snooping trust
    int range fa0/1-2
    no ip dhcp snooping trust
    ip dhcp snooping limit rate 10
ip dhcp snooping database flash:dhcp-
    snooping-database
no ip dhcp snooping information option
```

### ■ A-SW1

```
ip dhcp snooping
ip dhcp snooping vlan 1
ip dhcp snooping vlan 10
ip dhcp snooping vlan 20
ip dhcp snooping vlan 30
ip dhcp snooping vlan 40
    int rang gig 0/1-2
    ip dhcp snooping trust
    int rang fa0/1-2
    no ip dhcp snooping trust
    ip dhcp snooping limit rate 10
    exit
ip dhcp snooping database flash:dhcp-
    snooping-database
ip dhcp snooping information option
```

- DHCP Snooping was enabled to protect the network from rogue DHCP servers. This prevents devices from receiving incorrect IP configurations from unauthorized DHCP servers.



## ■ Dynamic ARP Inspection (DAI):

### ■ A-SW1

```
ip arp inspection vlan 1
ip arp inspection vlan 10
ip arp inspection vlan 20
ip arp inspection vlan 30
ip arp inspection vlan 40
    int rang gig0/1-2
    ip arp inspection trust
    int rang fa0/1-2
no ip arp inspection trust
ip arp inspection limit rate 15
```

### ■ A-SW2

```
ip arp inspection vlan 1
ip arp inspection vlan 10
ip arp inspection vlan 20
ip arp inspection vlan 30
ip arp inspection vlan 40
    int rang gig0/1-2
    ip arp inspection trust
    int rang fa0/1-2
no ip arp inspection trust
ip arp inspection limit rate 15
```

- DAI was configured to prevent ARP spoofing attacks, ensuring that only legitimate ARP replies are processed by network devices.

## ■ Storm Control:

### ■ A-SW1

```
int rang fa0/1-2
storm-control broadcast level 10.00
storm-control multicast level 5.00
storm-control unicast level 5.00
    storm-control action trap
    storm-control action shutdown
```

### ■ A-SW2

```
int rang fa0/1-2
storm-control broadcast level 10.00
storm-control multicast level 5.00
storm-control unicast level 5.00
    storm-control action trap
    storm-control action shutdown
```

- Storm Control was implemented to prevent broadcast, multicast, or unicast storms on the network, which could overwhelm network resources and degrade performance.



## ■ VLAN Hopping Prevention:

■ A-SW1  
int fa0/1  
switchport nonegotiate

■ A-SW2  
int fa0/1  
switchport nonegotiate

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





# CONCLUSION

This network infrastructure offers a scalable, secure, and efficient solution tailored to the organization's present and future requirements. It leverages advanced routing to ensure reliable and high-performance connectivity, while secure wireless communication supports mobility without compromising data protection. Robust security measures, VLAN segmentation, and intrusion prevention systems, help safeguard the network against both internal threats. Designed with flexibility and resilience in mind, this setup ensures continuous availability, protects critical resources, and provides a solid foundation for future expansion and integration of emerging technologies.



# THANK YOU FOR YOUR ATTENTION

Sayed Ahmed Sayed  
Yousef Mohamed Ahmed  
Ismail Abdallah Azab  
Ahmed Ashraf Ali  
Essam Hemida Hassan