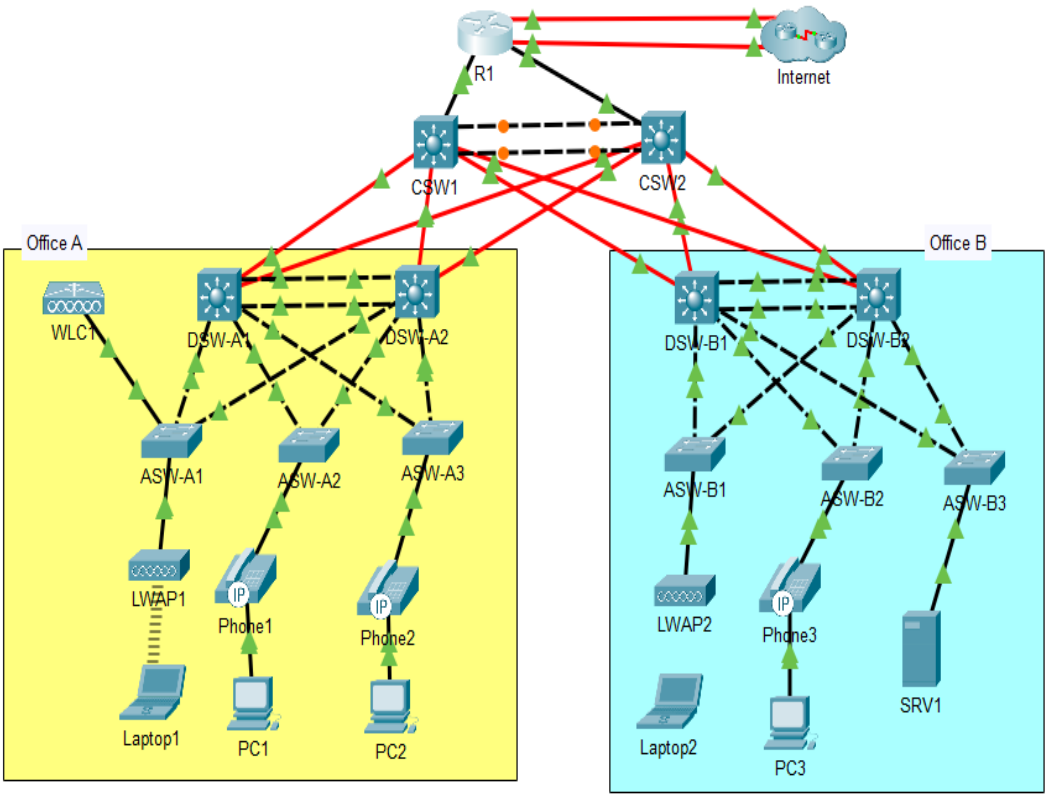
# Enterprise Network

This report documents the complete design, configuration, and implementation of a multi-site enterprise network based on the provided Packet Tracer project. The network features dual ISP connectivity, a hierarchical three-layer design (Core, Distribution, Access), VLAN segmentation, redundant gateways with HSRP, dynamic routing with OSPF, Layer 2/3 EtherChannels, IPv4/IPv6 addressing, and comprehensive security and network services. All configurations follow industry best practices and align with the detailed technical specifications provided.



**Part 1: Initial Device Setup**

Objective: Establish basic device identity, secure access, and console management.

I configured unique hostnames on each device to provide clear identification and simplify troubleshooting in a multi-device environment. From an infrastructure perspective, this allows network administrators to quickly identify device roles and locations during management or emergency situations. I implemented encrypted enable secrets and local user authentication to prevent unauthorized access to network devices, which is crucial for maintaining network integrity. The console line configuration with inactivity timeout ensures that idle management sessions don't become security vulnerabilities while synchronous logging provides clean output for configuration tasks.

Configuration Details:

1.1 Hostname Configuration:
Each device was configured with a unique hostname corresponding to its role and location (e.g., R1, CSW1, DSW-A1, ASW-A1).

```
# ASW, DSW, CSW and Router
hostname [hostname]
```

1.2-1.4 Security and Console Access:

- Enable Secret: Configured using Type 5 (MD5) hashing on older devices (R1, ASW) and Type 9 (scrypt) on newer platforms (CSW, DSW) as per capability.
- Local User Account: Created user cisco with secret ccna using corresponding hash types.
- Console Line: Configured for local authentication, 30-minute exec timeout, and synchronous logging.

```
# R1 and ASW (Access Switches)
enable secret jeremysitlab
```

```
username cisco secret ccna
line console 0
  login local
  exec-timeout 30
  logging synchronous
```

```
# CSW (Core Switches) And DSW (Distribution Switches)
enable algorithm-type scrypt secret jeremysitlab
username cisco algorithm-type scrypt secret ccna
line console 0
  login local
  exec-timeout 30
  logging synchronous
```

```
# Other helpful Command
write
write memory
copy running-config startup-config
show running-config
show running-config | include secret
```

**Part 2: VLANs and Layer-2 EtherChannel**

Objective: Implement VLAN segmentation, trunking, VTP for VLAN propagation, and redundant Layer-2 links.

I implemented VLAN segmentation to logically separate different types of network traffic (data, voice, management, wireless) which enhances security and performance by isolating broadcast domains. From an infrastructure perspective, this prevents a security breach in one department from easily spreading to others and optimizes network performance by reducing unnecessary traffic. I configured EtherChannel between distribution switches to combine multiple physical links into a single logical connection, providing increased bandwidth and redundancy if individual links fail. VTP was deployed to simplify VLAN management across multiple switches by allowing centralized configuration that automatically propagates to other switches in the domain.

Configuration Details:

2.1-2.2 Layer-2 EtherChannel:

- Office A (DSW-A1 & DSW-A2): Cisco-proprietary PAgP with desirable mode.
- Office B (DSW-B1 & DSW-B2): Open-standard LACP with active mode.

```
# DSW-A1 and DSW-A2
Interface range g1/0/4-5
  channel-protocol pagp
  channel-group 1 mode desirable
```

```
# DSW-B1 and DSW-B2
Interface range g1/0/4-5
  channel-protocol lacp
  channel-group 1 mode active
```

```
# Other helpful Command
```

```
show etherchannel summary
show cdp neighbors
```

2.3 Trunk Configuration:

All Distribution-to-Access links configured as trunks with:

- DTP disabled (switchport nonegotiate)
- Native VLAN 1000 (unused)
- VLAN pruning per office specifications

```
# DSW-A1, DSW-A2
interface range g1/0/1-3
  switchport mode trunk
  switchport nonegotiate
  switchport trunk native vlan 1000
  switchport trunk allowed vlan 10,20,40,99
interface po1
  switchport mode trunk
  switchport nonegotiate
  switchport trunk native vlan 1000
  switchport trunk allowed vlan 10,20,40,99
```

```
# ASW-A1, ASW-A2, ASW-A3
interface range g0/1-2
  switchport mode trunk
  switchport nonegotiate
  switchport trunk native vlan 1000
  switchport trunk allowed vlan 10,20,40,99
```

```
# DSW-B1, DSW-B2
interface range g1/0/1-3
  switchport mode trunk
  switchport nonegotiate
  switchport trunk native vlan 1000
  switchport trunk allowed vlan 10,20,30,99
interface po1
  switchport mode trunk
  switchport nonegotiate
  switchport trunk native vlan 1000
  switchport trunk allowed vlan 10,20,30,99
```

```
# ASW-B1, ASW-B2, ASW-B3
interface range g0/1-2
  switchport mode trunk
  switchport nonegotiate
  switchport trunk native vlan 1000
  switchport trunk allowed vlan 10,20,30,99
```

2.4 VTP Configuration:

- VTP Servers: DSW-A1 (Office A) and DSW-B1 (Office B)
- VTP Domain: JeremysITLab
- VTP Version: 2
- VTP Clients: All Access switches

```
# DSW-A1
vtp mode server
vtp domain JeremysITLab
```

```
vtp version 2
```

```
# ASW-A1, ASW-A2, ASW-A3
vtp mode client
```

```
# DSW-B1
vtp mode server
vtp domain JeremysITLab
vtp version 2
```

```
# ASW-B1, ASW-B2, ASW-B3
vtp mode client
```

```
# Other helpful Command
show vtp status
```

2.5-2.6 VLAN Creation:
VLANs created on VTP servers and propagated to clients.

```
# DSW-A1
vlan 10
  name PCs
vlan 20
  name Phones
vlan 40
  name Wi-Fi
vlan 99
  name Management
```

```
# DSW-B1
vlan 10
  name PCs
vlan 20
  name Phones
vlan 40
  name Servers
vlan 99
  name Management
```

```
# Other helpful Command
show vlan brief
```

2.7 Access Port Configuration:

Ports configured for specific devices with DTP disabled.

```
# ASW-A1, ASW-B1
interface f0/1
  switchport mode access
  switchport nonegotiate
  switchport access vlan 99
```

```
# ASW-A2, ASW-A3, ASW-B2
interface f0/1
  switchport mode access
  switchport nonegotiate
  switchport access vlan 10
  switchport voice vlan 20
```

```
# ASW-B3
interface f0/1
  switchport mode access
  switchport nonegotiate
  switchport access vlan 30
```

2.8 WLC Trunk Configuration:
ASW-A1 interface to WLC1 configured as trunk for Wi-Fi and Management VLANs.

```
# ASW-A1
interface f0/2
  switchport mode trunk
  switchport trunk allowed vlan 40, 99
  switchport trunk native vlan 99
  switchport nonegotiate
```

2.9 Unused Port Management:
All unused ports administratively disabled on Distribution and Access switches.

```
# DSW-A1, DSW-A2, DSW-B1, DSW-B2
show interfaces status
interface range g1/0/6-24, g1/1/3-4
  shutdown
```

```
# ASW-A1
show interfaces status
Interface range f0/3-24
  shutdown
```

```
# ASW-A2, ASW-A3, ASW-B1, ASW-B2, ASW-B3
show interfaces status
Interface range f0/2-24
  Shutdown
```

**Part 3: IP Addressing, Layer-3 EtherChannel, and HSRP**

Objective: Configure IP addressing, Layer-3 connectivity, and gateway redundancy.

I assigned hierarchical IP addresses following a structured scheme to enable efficient routing and simplify network management. From an infrastructure perspective, this organized addressing allows for easy subnet identification, efficient route summarization, and straightforward troubleshooting. I implemented Layer-3 EtherChannel between core switches to create a high-bandwidth backbone that aggregates multiple links into a single logical interface, providing both increased throughput and redundancy. HSRP was configured to provide gateway redundancy, ensuring continuous network availability by automatically failing over to backup routers when primary gateways become unavailable.

Configuration Details:

```
# R1
interface range g0/0/0, g0/1/0
  ip address dhcp
  no shutdown
interface g0/0
  ip address 10.0.0.33 255.255.255.252
  no shutdown
interface g0/1
  ip address 10.0.0.37 255.255.255.252
  no shutdown
interface loopback 0
  ip address 10.0.0.76 255.255.255.255
  no shutdown
```

3.2 IP Routing Enabled:

```
# CSW and DSW
configure terminal
ip routing
```

3.3-3.5 Layer-3 EtherChannel and Addressing:

```
Part 3, Step 3
# CSW1
interface range g1/0/2-3
  no switchport
  channel-group 1 mode desirable
interface po1
  ip address 10.0.0.41 255.255.255.252
```

```
# CSW2
interface range g1/0/2-3
  no switchport
  channel-group 1 mode desirable
interface po1
  ip address 10.0.0.42 255.255.255.252
ping 10.0.0.41
```

```
Part 3, Step 4
# CSW1
interface g1/0/1
  no switchport
  ip address 10.0.0.34 255.255.255.252
```

```
interface g1/1/1
  no switchport
  ip address 10.0.0.45 255.255.255.252
interface g1/1/2
  no switchport
  ip address 10.0.0.49 255.255.255.252
interface g1/1/3
  no switchport
  ip address 10.0.0.53 255.255.255.252
interface g1/1/4
  no switchport
  ip address 10.0.0.57 255.255.255.252
interface loopback 0
  ip address 10.0.0.77 255.255.255.255
interface range g1/0/4-24
  shutdown
```

```
Part 3, Step 5
# CSW2
interface g1/0/1
  no switchport
  ip address 10.0.0.38 255.255.255.252
interface g1/1/1
  no switchport
  ip address 10.0.0.61 255.255.255.252
interface g1/1/2
  no switchport
  ip address 10.0.0.65 255.255.255.252
```

```
interface g1/1/3
  no switchport
  ip address 10.0.0.69 255.255.255.252
interface g1/1/4
  no switchport
  ip address 10.0.0.73 255.255.255.252
interface loopback 0
  ip address 10.0.0.78 255.255.255.255
interface range g1/0/4-24
  shutdown
```

3.6-3.9 Distribution Switch Addressing:
Each Distribution switch configured with:

- Uplink interfaces to Core switches
- Loopback addresses for management and OSPF RID

```
Part 3, Step 6
# DSW-A1
interface g1/1/1
  no switchport
  ip address 10.0.0.46 255.255.255.252
interface g1/1/2
  no switchport
  ip address 10.0.0.62 255.255.255.252
interface loopback 0
  ip address 10.0.0.79 255.255.255.255
```

```
Part 3, Step 7
# DSW-A2
interface g1/1/1
  no switchport
  ip address 10.0.0.50 255.255.255.252
interface g1/1/2
  no switchport
  ip address 10.0.0.66 255.255.255.252
interface loopback 0
  ip address 10.0.0.80 255.255.255.255
```

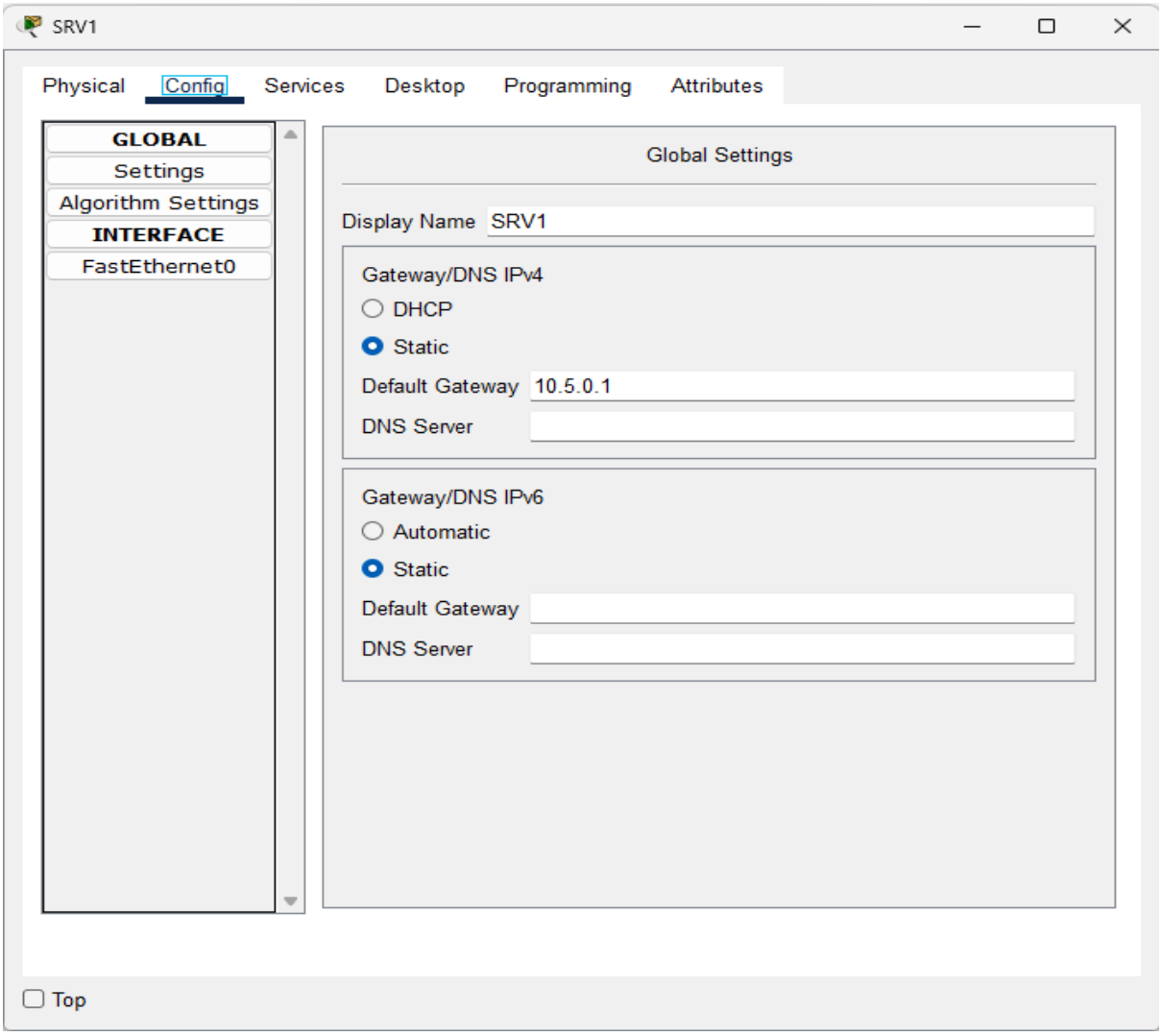
```
Part 3, Step 8
# DSW-B1
interface g1/1/1
  no switchport
  ip address 10.0.0.54 255.255.255.252
interface g1/1/2
  no switchport
  ip address 10.0.0.70 255.255.255.252
interface loopback 0
  ip address 10.0.0.81 255.255.255.255
```

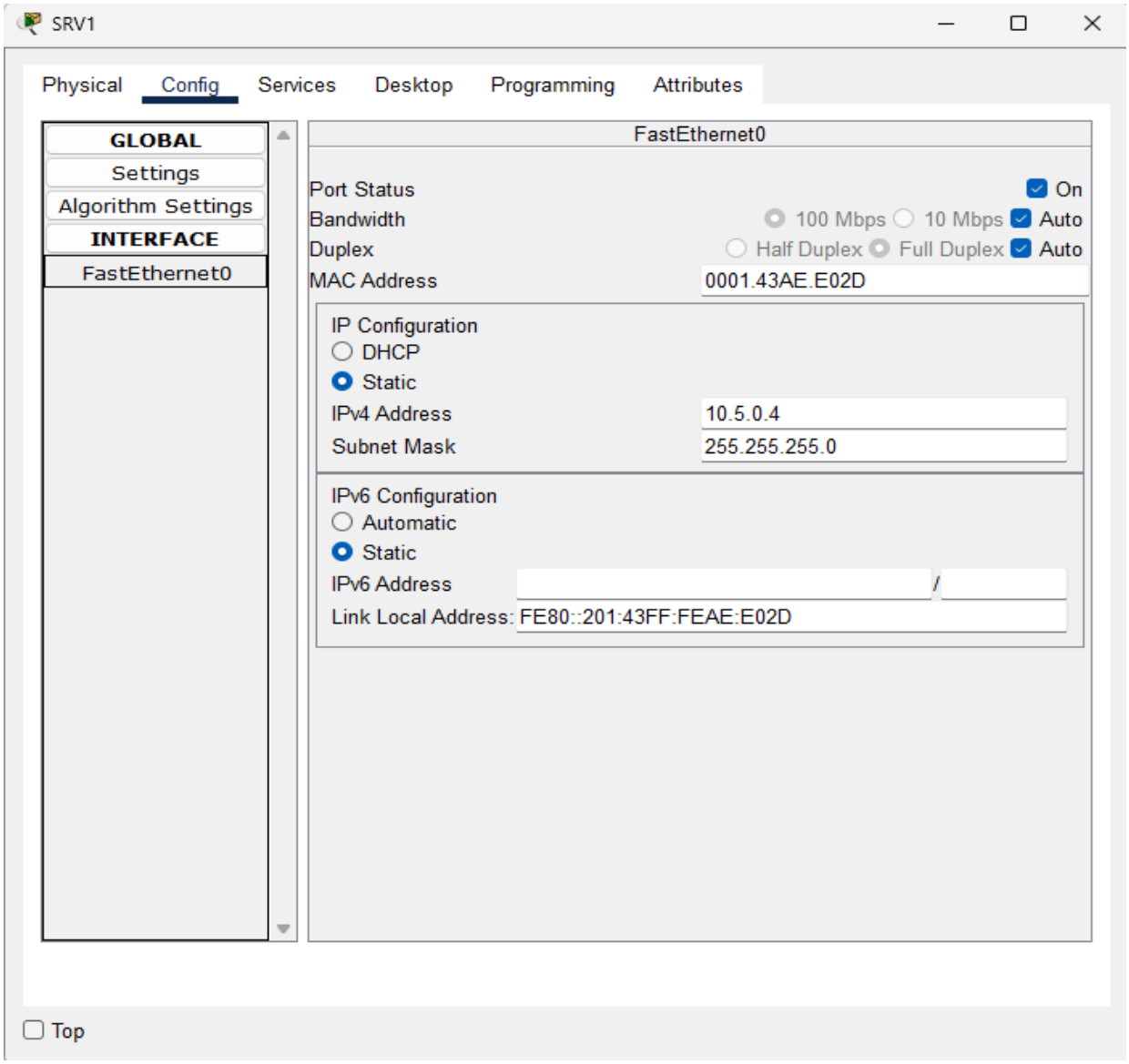
```
Part 3, Step 9
# DSW-B2
interface g1/1/1
  no switchport
  ip address 10.0.0.58 255.255.255.252
```

```
interface g1/1/2
  no switchport
  ip address 10.0.0.74 255.255.255.252
interface loopback 0
  ip address 10.0.0.82 255.255.255.255
```

3.10 SRV1 Manual Configuration:

- IP Address: 10.5.0.4/24
- Default Gateway: 10.5.0.1
- DNS Server: Self-referencing (10.5.0.4)






3.11 Access Switch Management:

Management IPs configured on VLAN 99 interfaces with appropriate default gateways.

```
# ASW-A1
ip default-gateway 10.0.0.1
interface vlan 99
  ip address 10.0.0.4 255.255.255.240
# ASW-A2
ip default-gateway 10.0.0.1
```

```
interface vlan 99
  ip address 10.0.0.5 255.255.255.240
# ASW-A3
ip default-gateway 10.0.0.1
interface vlan 99
  ip address 10.0.0.6 255.255.255.240
# ASW-B1
ip default-gateway 10.0.0.17
interface vlan 99
  ip address 10.0.0.20 255.255.255.240
# ASW-B2
ip default-gateway 10.0.0.17
interface vlan 99
  ip address 10.0.0.21 255.255.255.240
# ASW-B3
ip default-gateway 10.0.0.17
interface vlan 99
  ip address 10.0.0.22 255.255.255.240
```

3.12-3.19 HSRPv2 Configuration:
Gateway redundancy configured with load balancing across Distribution switches.

```
Part 3, Step 12
# DSW-A1
int vlan 99
  ip address 10.0.0.2 255.255.255.240
  standby version 2
  standby 1 ip 10.0.0.1
```

```
  standby 1 priority 105
  standby 1 preempt
# DSW-A2
int vlan 99
  ip address 10.0.0.3 255.255.255.240
  standby version 2
  standby 1 ip 10.0.0.1
```

```
Part 3, Step 13
# DSW-A1
int vlan 10
  ip address 10.1.0.2 255.255.255.0
  standby version 2
  standby 2 ip 10.1.0.1
  standby 2 priority 105
  standby 2 preempt

# DSW-A2
int vlan 10
  ip address 10.1.0.3 255.255.255.0
  standby version 2
  standby 2 ip 10.1.0.1
```

```
Part 3, Step 14
# DSW-A1
int vlan 20
  ip address 10.2.0.2 255.255.255.0
  standby version 2
```

```
  standby 3 ip 10.2.0.1
# DSW-A2
int vlan 20
  ip address 10.2.0.3 255.255.255.0
  standby version 2
  standby 3 ip 10.2.0.1
  standby 3 priority 105
  standby 3 preempt
```

```
Part 3, Step 15
# DSW-A1
int vlan 40
  ip address 10.6.0.2 255.255.255.0
  standby version 2
  standby 4 ip 10.6.0.1
# DSW-A2
int vlan 40
  ip address 10.6.0.3 255.255.255.0
  standby version 2
  standby 4 ip 10.6.0.1
  standby 4 priority 105
  standby 4 preempt
```

```
Part 3, Step 16
# DSW-B1
int vlan 99
  ip address 10.0.0.18 255.255.255.240
  standby version 2
```

```
  standby 1 ip 10.0.0.17
  standby 1 priority 105
  standby 1 preempt
# DSW-B2
int vlan 99
  ip address 10.0.0.19 255.255.255.240
  standby version 2
  standby 1 ip 10.0.0.17
```

```
Part 3, Step 17
# DSW-B1
int vlan 10
  ip address 10.3.0.2 255.255.255.0
  standby version 2
  standby 2 ip 10.3.0.1
  standby 2 priority 105
  standby 2 preempt
# DSW-B2
int vlan 10
  ip address 10.3.0.3 255.255.255.0
  standby version 2
  standby 2 ip 10.3.0.1
```

```
Part 3, Step 18
# DSW- B1
int vlan 20
  ip address 10.4.0.2 255.255.255.0
```

```
  standby version 2
  standby 3 ip 10.4.0.1
# DSW- B2
int vlan 20
  ip address 10.4.0.3 255.255.255.0
  standby version 2
  standby 3 ip 10.4.0.1
  standby 3 priority 105
  standby 3 preempt
```

```
Part 3, Step 19
# DSW-A1
int vlan 30
  ip address 10.5.0.2 255.255.255.0
  standby version 2
  standby 4 ip 10.5.0.1
# DSW-A2
int vlan 30
  ip address 10.5.0.3 255.255.255.0
  standby version 2
  standby 4 ip 10.5.0.1
  standby 4 priority 105
  standby 4 preempt
```

```
# Other helpful Command
show ip interface brief
```

**Part 4: Rapid Spanning Tree Protocol**

Objective: Configure loop prevention with Rapid PVST+ and optimize convergence.

I deployed Rapid PVST+ to prevent Layer-2 loops while providing fast convergence during network topology changes. From an infrastructure perspective, this ensures network stability by blocking redundant paths that could cause broadcast storms while maintaining backup paths for redundancy. I aligned root bridge selection with HSRP active routers to optimize traffic paths and avoid suboptimal routing that could cause congestion on certain links. PortFast and BPDU Guard configurations accelerated client connectivity while protecting against accidental switching loop creation from end-user devices.

Configuration Details:

```
# ASW and DSW
spanning-tree mode rapid-pvst
# DSW-A1
spanning-tree vlan 10,99 priority 0
spanning-tree vlan 20,40 priority 4096
do show spanning-tree vlan 10
# DSW-A2
spanning-tree vlan 10,99 priority 4096
spanning-tree vlan 20,40 priority 0
# DSW-B1
spanning-tree vlan 10,99 priority 0
spanning-tree vlan 20,30 priority 4096
do show spanning-tree vlan 10
# DSW-B2
spanning-tree vlan 10,99 priority 4096
spanning-tree vlan 20,30 priority 0
```

4.2 PortFast and BPDU Guard:

```
# ASW-A1
int f0/1
  spanning-tree portfast
  spanning-tree bpduguard enable
int f0/2
  spanning-tree portfast trunk
  spanning-tree bpduguard enable
# ASW-A2, ASW-A3, ASW-B1, ASW-B2, ASW-A3
int f0/1
  spanning-tree portfast
  spanning-tree bpduguard enable
do write
```

```
# Other helpful Command
show sapanning-tree
show spanning-tree vlan 10
```

**Part 5: Static and Dynamic Routing**

Objective: Establish full IP connectivity with OSPF and redundant Internet routes.

I implemented OSPF as the dynamic routing protocol to automatically adapt to network changes and failures without manual intervention. From an infrastructure perspective, this provides self-healing capabilities where the network automatically finds alternative paths when links or devices fail, ensuring continuous connectivity. I configured static default routes with a floating backup to provide reliable Internet connectivity through dual ISPs with automatic failover capabilities. The OSPF hierarchy with all devices in Area 0 simplified routing while maintaining the scalability needed for future network expansion.

Configuration Details:

5.1 OSPF Configuration:

```
# R1
router ospf 1
  router-id 10.0.0.76
  passive-interface loopback0
interface loopback0
  ip ospf 1 area 0
interface range g0/0-1
  ip ospf 1 area 0
  ip ospf network point-to-point
do write
```

```
# CSW-A1
router ospf 1
  router-id 10.0.0.77
  passive-interface loopback0
  network 10.0.0.41 0.0.0.0 area 0
  network 10.0.0.34 0.0.0.0 area 0
```

```
  network 10.0.0.45 0.0.0.0 area 0
  network 10.0.0.49 0.0.0.0 area 0
  network 10.0.0.53 0.0.0.0 area 0
  network 10.0.0.57 0.0.0.0 area 0
  network 10.0.0.77 0.0.0.0 area 0

interface range g1/0/1, g1/1/1-4
  ip ospf network point-to-point
do write
```

```
# CSW-A2
router ospf 1
  router-id 10.0.0.78
  passive-interface loopback0
  network 10.0.0.42 0.0.0.0 area 0
  network 10.0.0.38 0.0.0.0 area 0
  network 10.0.0.61 0.0.0.0 area 0
  network 10.0.0.65 0.0.0.0 area 0
  network 10.0.0.69 0.0.0.0 area 0
  network 10.0.0.73 0.0.0.0 area 0
  network 10.0.0.78 0.0.0.0 area 0
interface range g1/0/1, g1/1/1-4
  ip ospf network point-to-point
do write
```

```
# DSW-A1
router ospf 1
  router-id 10.0.0.79
```

```
  passive-interface loopback0
  passive-interface vlan 10
  passive-interface vlan 20
  passive-interface vlan 40
  network 10.0.0.46 0.0.0.0 area 0
  network 10.0.0.62 0.0.0.0 area 0
  network 10.0.0.79 0.0.0.0 area 0
  network 10.1.0.2 0.0.0.0 area 0
  network 10.2.0.2 0.0.0.0 area 0
  network 10.0.0.2 0.0.0.0 area 0
  network 10.6.0.2 0.0.0.0 area 0
interface range g1/1/1-2
  ip ospf network point-to-point
do write
```

```
# DSW-A2
router ospf 1
  router-id 10.0.0.80
  passive-interface loopback0
  passive-interface vlan 10
  passive-interface vlan 20
  passive-interface vlan 40
  network 10.0.0.50 0.0.0.0 area 0
  network 10.0.0.66 0.0.0.0 area 0
  network 10.0.0.80 0.0.0.0 area 0
  network 10.1.0.3 0.0.0.0 area 0
  network 10.2.0.3 0.0.0.0 area 0
```

```
  network 10.0.0.3 0.0.0.0 area 0
  network 10.6.0.3 0.0.0.0 area 0
interface range g1/1/1-2
  ip ospf network point-to-point
do write
```

```
# DSW-B1
router ospf 1
  router-id 10.0.0.81
  passive-interface loopback0
  passive-interface vlan 10
  passive-interface vlan 20
  passive-interface vlan 30
  network 10.0.0.54 0.0.0.0 area 0
  network 10.0.0.70 0.0.0.0 area 0
  network 10.0.0.81 0.0.0.0 area 0
  network 10.3.0.2 0.0.0.0 area 0
  network 10.4.0.2 0.0.0.0 area 0
  network 10.5.0.2 0.0.0.0 area 0
  network 10.0.0.18 0.0.0.0 area 0
interface range g1/1/1-2
  ip ospf network point-to-point
do write
```

```
# DSW-B2
router ospf 1
  router-id 10.0.0.82
```

```
  passive-interface loopback0
  passive-interface vlan 10
  passive-interface vlan 20
  passive-interface vlan 30
  network 10.0.0.58 0.0.0.0 area 0
  network 10.0.0.74 0.0.0.0 area 0
  network 10.0.0.82 0.0.0.0 area 0
  network 10.3.0.3 0.0.0.0 area 0
  network 10.4.0.3 0.0.0.0 area 0
  network 10.5.0.3 0.0.0.0 area 0
  network 10.0.0.19 0.0.0.0 area 0
interface range g1/1/1-2
  ip ospf network point-to-point
do write
```

5.2 Static Default Routes and OSPF Redistribution:

```
# R1
do ping 203.0.113.1
do ping 203.0.113.5
ip route 0.0.0.0 0.0.0.0 203.0.113.1
ip route 0.0.0.0 0.0.0.0 203.0.113.5 2
do show ip route
router ospf 1
  default-information originate
# Other helpful Command
show ip ospf
show ip ospf interface
```

```
show ip ospf interface [interface]
show ip ospf interface brief
show ip ospf database
show ip ospf neighbor
show ip route
show ip interface brief | exclude unassigned
```

**Part 6: Network Services**

Objective: Implement DHCP, DNS, NTP, SNMP, Syslog, FTP, SSH, and NAT services.

Rationale and Infrastructure Perspective: I configured DHCP services to automate IP address management for hundreds of devices, reducing administrative overhead and preventing address conflicts. From an infrastructure perspective, this centralized approach ensures consistent network configuration and simplifies device onboarding. I implemented DNS for name resolution, NTP for time synchronization across all devices, and Syslog for centralized logging, which are essential for troubleshooting and maintaining operational consistency. SSH replaced insecure Telnet for encrypted remote management, while NAT enabled Internet access for internal users while conserving public IP addresses.

Configuration Details:

6.1 DHCP Server Configuration (R1):

```
# R1
ip dhcp excluded-address 10.0.0.1 10.0.0.10
ip dhcp excluded-address 10.1.0.1 10.1.0.10
ip dhcp excluded-address 10.2.0.1 10.2.0.10
ip dhcp excluded-address 10.0.0.17 10.0.0.26
ip dhcp excluded-address 10.3.0.1 10.3.0.10
ip dhcp excluded-address 10.4.0.1 10.4.0.10
ip dhcp excluded-address 10.6.0.1 10.6.0.10
```

```
ip dhcp pool A-Mgmt
  network 10.0.0.0 255.255.255.240
  default-router 10.0.0.1
  domain-name jeremysitlab.com
  dns-server 10.5.0.4
  option 43 ip 10.0.0.7
```

```
ip dhcp pool A-PC
  network 10.1.0.0 255.255.255.0
  default-router 10.1.0.1
  domain-name jeremysitlab.com
  dns-server 10.5.0.4
```

```
ip dhcp pool A-Phone
  network 10.2.0.0 255.255.255.0
  default-router 10.2.0.1
  domain-name jeremysitlab.com
  dns-server 10.5.0.4
```

```
ip dhcp pool B-Mgmt
  network 10.0.0.16 255.255.255.240
  default-router 10.0.0.17
  domain-name jeremysitlab.com
  dns-server 10.5.0.4
  option 43 ip 10.0.0.7
```

```
ip dhcp pool B-PC
  network 10.3.0.0 255.255.255.0
  default-router 10.3.0.1
  domain-name jeremysitlab.com
  dns-server 10.5.0.4
```

```
ip dhcp pool B-Phone
  network 10.4.0.0 255.255.255.0
```

```
  default-router 10.4.0.1
  domain-name jeremysitlab.com
  dns-server 10.5.0.4
```

```
ip dhcp pool Wi-Fi
  network 10.6.0.0 255.255.255.0
  default-router 10.6.0.1
  domain-name jeremysitlab.com
  dns-server 10.5.0.4
```

6.2 DHCP Relay Configuration:

```
# DSW-A1, DSW-A2
interface vlan 10
  ip helper-address 10.0.0.76
interface vlan 20
  ip helper-address 10.0.0.76
interface vlan 40
  ip helper-address 10.0.0.76
interface vlan 99
  ip helper-address 10.0.0.76
```

```
# DSW-B1, DSW-B2
interface vlan 10
  ip helper-address 10.0.0.76
interface vlan 20
  ip helper-address 10.0.0.76
interface vlan 30
```

```
  ip helper-address 10.0.0.76
interface vlan 99
  ip helper-address 10.0.0.76
```

```
# Other helpful Command
do show ip dhcp binding
```

6.3-6.4 DNS Configuration:

- SRV1 DNS Records:

  google.com = 172.253.62.100

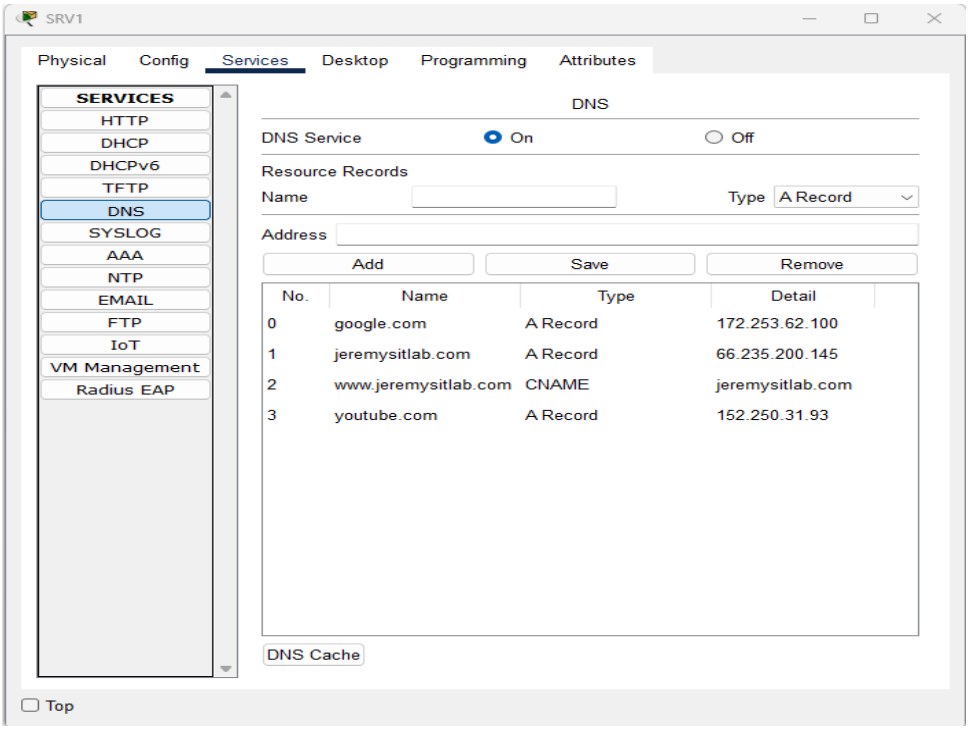
  youtube.com = 152.250.31.93

  jeremysitlab.com = 66.235.200.145

  www.jeremysitlab.com = jeremysitlab.com (CNAME)

- Device DNS Configuration:
  ip domain name jeremysitlab.com
  ip name-server 10.5.0.4

# SRV1



```
# PC1
ping 10.5.0.4
ping google.com
ping jeremysitlab.com
ping www.jeremysitlab.com
```

```
Part 6, Step 4
# R1, CSW, DSW, ASW
ip domain name jeremysitlab.com
ip name-server 10.5.0.4
```

6.5-6.6 NTP Configuration:

```
Part 6, Step 5
# R1
ntp master 5
ntp server 216.239.35.0
```

```
Part 6, Step 6
# R1
ntp authentication-key 1 md5 ccna
ntp trusted-key 1
```

```
# CSW, DSW, ASW
ntp authentication-key 1 md5 ccna
ntp trusted-key 1
ntp server 10.0.0.76 key 1
```

6.7 SNMP and Syslog:

```
# R1, CSW, DSW, ASW
snmp-server community SNMPSTRING ro
```

```
logging host 10.5.0.4
logging trap debugging
logging buffered 8192
```

```
# Other helpful Command
show logging
```

6.9 FTP IOS Upgrade:

```
# R1
ip ftp username cisco
ip ftp password cisco
ping 10.5.0.4
copy ftp flash
  10.5.0.4
  c2900-universalk9-mz.SPA.155-3.M4a.bin
do show flash
boot system flash:c2900-universalk9-mz.SPA.155-
3.M4a.bin
do write
do show version
do reload
do show version
delete flash:c2900-universalk9-mz.SPA.151-4.M4.bin
do show flash
```

```
# Other helpful Command
show file systems
```

6.10 SSH Configuration:

```
# R1, CSW, DSW, ASW
crypto key generate rsa
  4096
access-list 1 permit 10.1.0.0 0.0.0.255
do show ip ssh
ip ssh version 2
line vty 0 15
  access-class 1 in
  transport input ssh
  login local
  logging synchronous
```

6.11-6.12 NAT Configuration:

```
Part 6, Step 11
# R1
ip nat inside source static 10.5.0.4 203.0.113.113
interface range g0/0/0, g0/1/0
  ip nat outside
interface range g0/0-1
  ip nat inside
```

```
Part 6, Step 12
# R1
```

```
access-list 2 permit 10.1.0.0 0.0.0.255
access-list 2 permit 10.2.0.0 0.0.0.255
access-list 2 permit 10.3.0.0 0.0.0.255
access-list 2 permit 10.4.0.0 0.0.0.255
access-list 2 permit 10.6.0.0 0.0.0.255
```

```
ip nat pool POOL1 203.0.113.200 203.0.113.207 netmask
255.255.255.248
ip nat inside source list 2 pool POOL1 overload
```

```
int g0/0/0
  shutdown
router ospf 1
  no default-information originate
  default-information originate
do show ip route

int g0/0/0
  no shutdown
router ospf 1
  no default-information originate
  default-information originate
do show ip route
```

6.13 CDP/LLDP Configuration:

```
# R1, CSW, DSW, ASW
no cdp run
lldp run
```

```
# ASW
interface f0/1
  no lldp transmit
do write
```

**Part 7: Security Features**

Objective: Implement traffic filtering and Layer-2 security mechanisms.

I implemented extended ACLs to control traffic flow between different departments, enforcing security policies at the network edge where it's most efficient. From an infrastructure perspective, this prevents unauthorized communication between network segments while allowing legitimate business traffic. I configured Port Security to limit the number of MAC addresses on access ports, preventing unauthorized device connections and MAC flooding attacks. DHCP Snooping and Dynamic ARP Inspection protect against man-in-the-middle attacks by validating DHCP transactions and ARP messages, which are common attack vectors in enterprise networks.

Configuration Details:

7.1 Extended ACL for Inter-Office Traffic:

```
# DSW-A1, DSW-A2
ip access-list extended OfficeA_to_OfficeB
permit icmp 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255
deny ip 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255
permit ip any any

interface vlan 10
ip access-group OfficeA_to_OfficeB in
do write
```

7.2 Port Security:

```
# ASW-A1, ASW-B1, ASW-B3
interface f0/1
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security violation restrict
```

```
# ASW-A2, ASW-A3, ASW-B2
interface f0/1
  switchport port-security
  switchport port-security maximum 2
  switchport port-security mac-address sticky
  switchport port-security violation restrict
```

7.3 DHCP Snooping:

```
# ASW-A1
ip dhcp snooping
ip dhcp snooping vlan 10,20,40,99
no ip dhcp snooping information option
interface range g0/1-2
  ip dhcp snooping trust
interface f0/1
  ip dhcp snooping limit rate 15
interface f0/2
  ip dhcp snooping limit rate 100
do write
```

```
# ASW-A2, ASW-A3
ip dhcp snooping
ip dhcp snooping vlan 10,20,40,99
no ip dhcp snooping information option
interface range g0/1-2
  ip dhcp snooping trust
interface f0/1
```

```
  ip dhcp snooping limit rate 15
do write
```

```
# ASW-B1, ASW-B2, ASW-B3
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,99
no ip dhcp snooping information option
interface range g0/1-2
  ip dhcp snooping trust
interface f0/1
  ip dhcp snooping limit rate 15
do write
```

7.4 Dynamic ARP Inspection:

```
# ASW-A1, ASW-A2, ASW-A3
ip arp inspection vlan 10,20,40,99
ip arp inspection validate src-mac dst-mac ip
interface range g0/1-2
  ip arp inspection trust
do write
# ASW-B1, ASW-B2, ASW-B3
ip arp inspection vlan 10,20,30,99
ip arp inspection validate src-mac dst-mac ip
interface range g0/1-2
  ip arp inspection trust
do write
```

**Part 8: IPv6 Implementation**

Objective: Configure IPv6 addressing and routing for future migration.

I configured IPv6 addresses on core infrastructure to prepare for future protocol migration and support dual-stack operation during the transition period. From an infrastructure perspective, this ensures compatibility with IPv6-enabled devices and services as IPv4 addresses become increasingly scarce. I implemented IPv6 static routes to establish basic connectivity testing for the next-generation Internet protocol while maintaining full IPv4 functionality. This forward-looking implementation maintains network viability for the long term while providing a foundation for gradually adopting IPv6 as it becomes more prevalent.

Configuration Details:

8.1 IPv6 Addressing:

```
#R1
ipv6 unicast-routing
interface g0/0/0
  ipv6 address 2001:db8:a::2/64
interface g0/1/0
  ipv6 address 2001:db8:b::2/64
interface g0/0
  ipv6 address 2001:db8:a1::/64 eui-64
interface g0/1
  ipv6 address 2001:db8:a2::/64 eui-64
do show ipv6 interface brief
do write
```

```
# CSW1
ipv6 unicast-routing
interface g1/0/1
```

```
  ipv6 address 2001:db8:a1::/64 eui-64
interface po1
  ipv6 enable
do write

# CSW2
ipv6 unicast-routing
interface g1/0/1
  ipv6 address 2001:db8:a2::/64 eui-64
interface po1
  ipv6 enable
do write
```

8.2 IPv6 Static Routing:

```
#R1
ipv6 route ::/0 2001:db8:a::1
ipv6 route ::/0 g0/1/0 2001:db8:b::1 2
do write
```

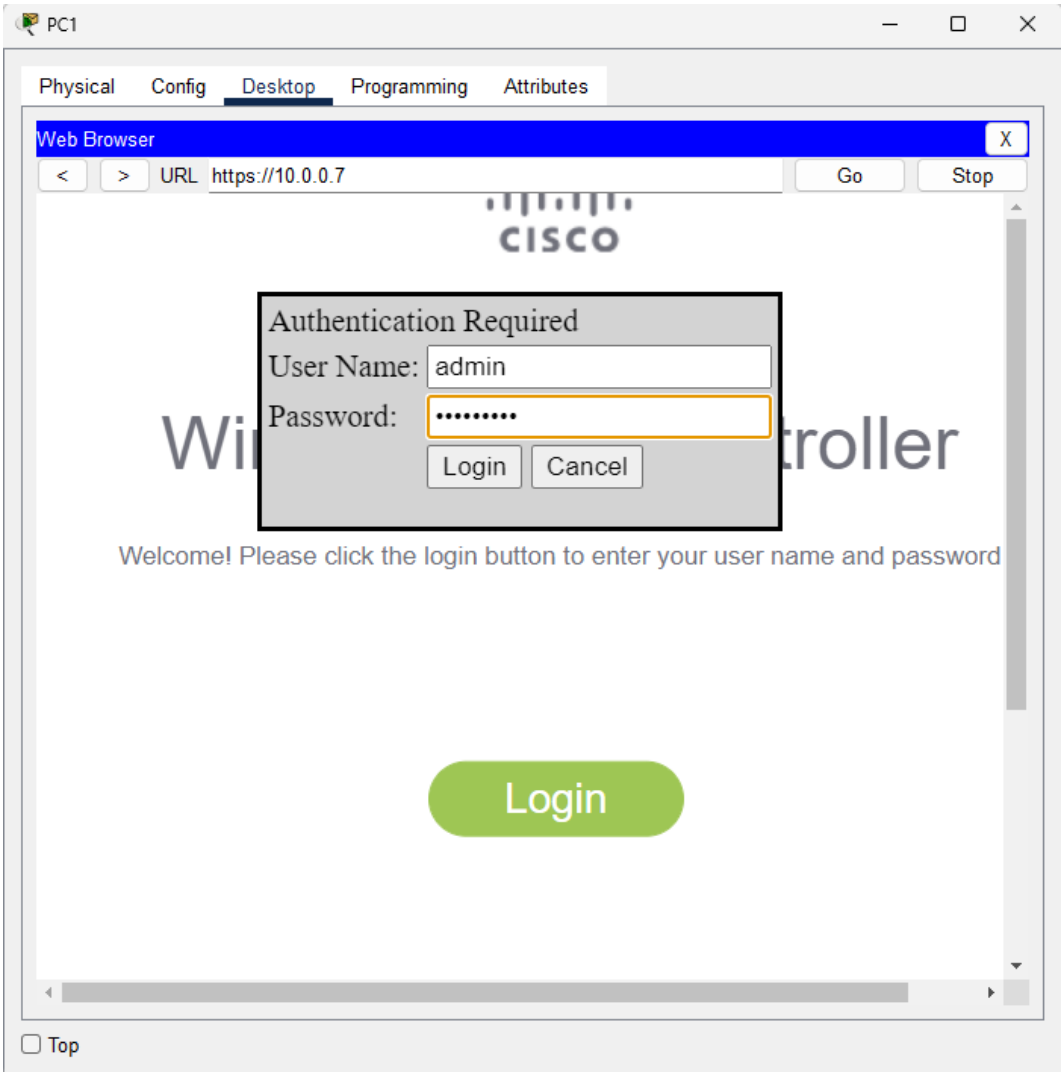
**Part 9: Wireless Configuration**

Objective: Configure WLC1 and wireless network for Wi-Fi access.

I integrated wireless infrastructure with the wired network through VLAN trunking to provide seamless connectivity between wired and wireless users. From an infrastructure perspective, this allows wireless traffic to be properly segmented and secured while maintaining access to necessary network resources. I configured the wireless controller to centralize management of access points, simplifying configuration and monitoring of the wireless network. WPA2 encryption was implemented to secure wireless communications against eavesdropping, which is essential for protecting sensitive data transmitted over the air.

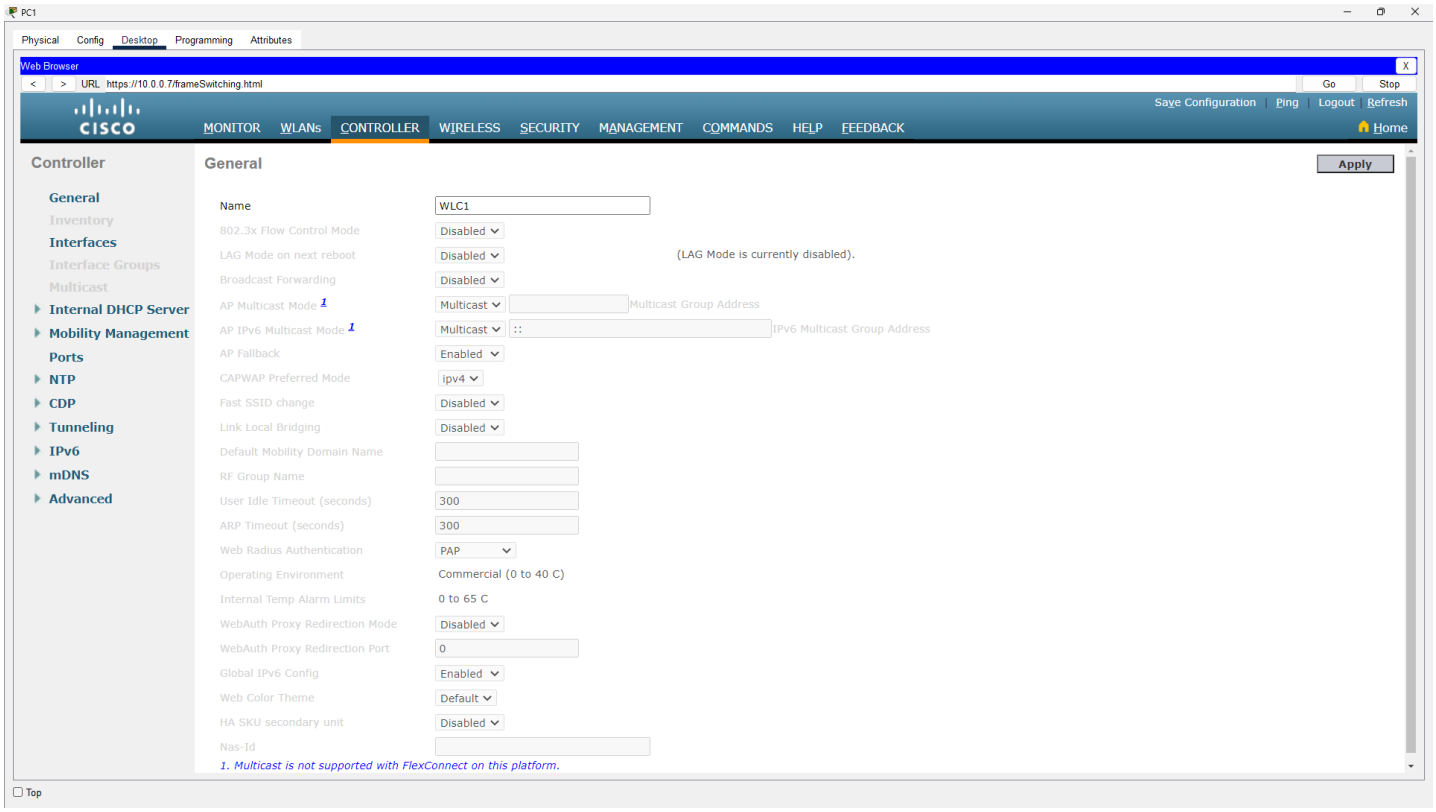
Configuration Details:

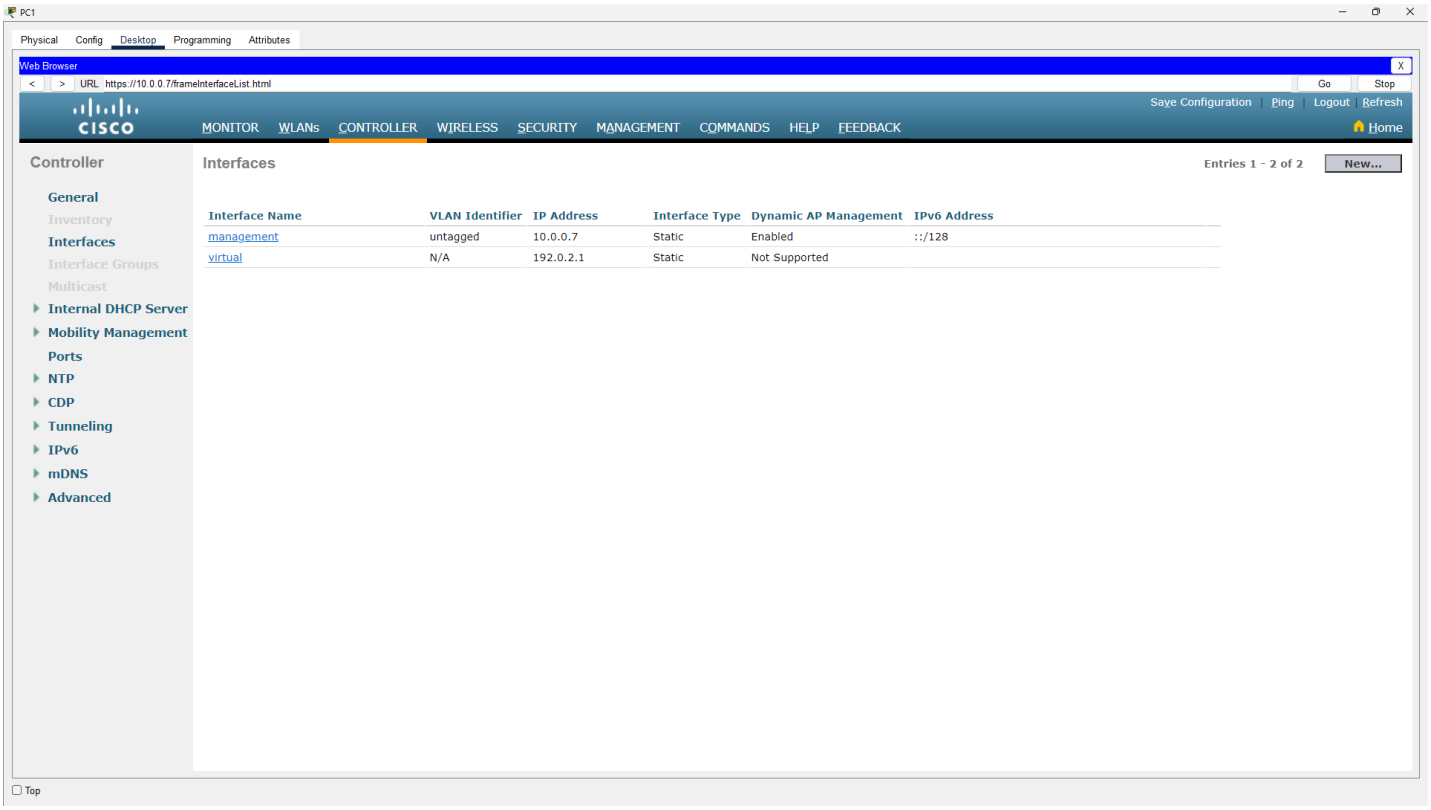
9.1 WLC1 Initial Access:

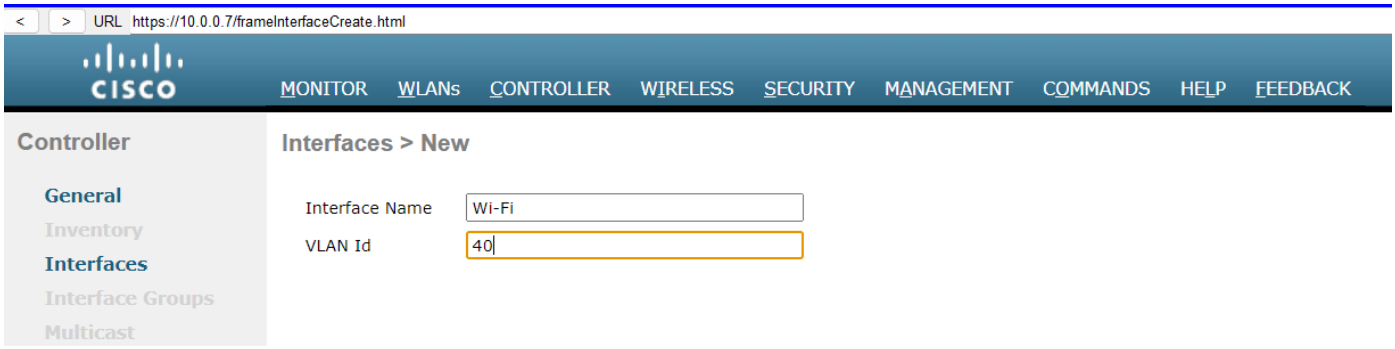


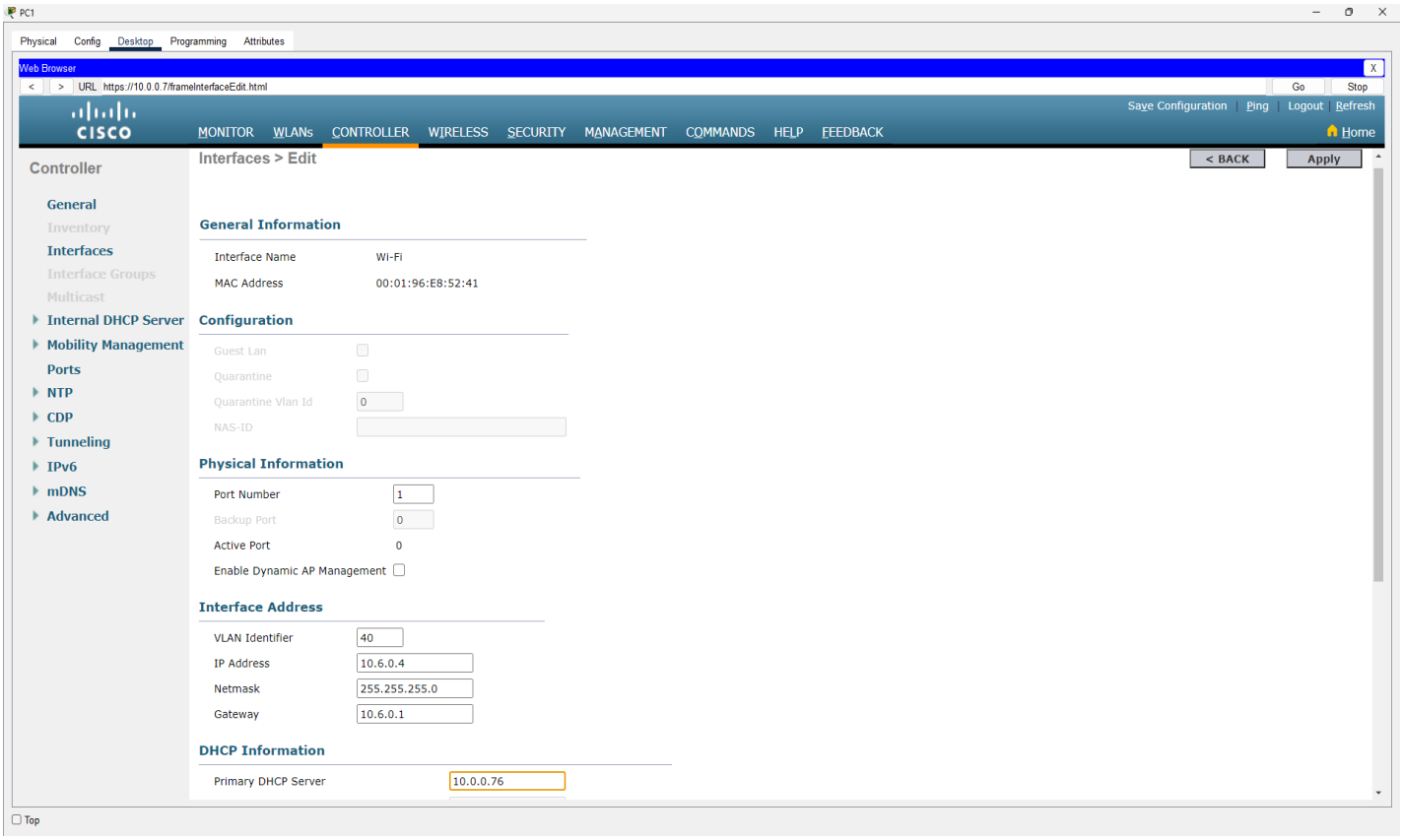
9.2 Dynamic Interface Configuration:

- Interface Name: Wi-Fi
- VLAN: 40
- Port Number: 1
- IP Address: 10.6.0.4/24 (Corrected from video mistake of .2)
- Gateway: 10.6.0.1
- DHCP Server: 10.0.0.76


PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.0.0.7/frameSwitching.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Tunneling
IPv6
mDNS
Advanced
General
Apply
Name
WLC1
802.3x Flow Control Mode
Disabled
LAG Mode on next reboot
Disabled
(LAG Mode is currently disabled).
Broadcast Forwarding
Disabled
AP Multicast Mode 1
Multicast
Multicast Group Address
AP IPv6 Multicast Mode 1
Multicast
::
IPv6 Multicast Group Address
AP Fallback
Enabled
CAPWAP Preferred Mode
ipv4
Fast SSID change
Disabled
Link Local Bridging
Disabled
Default Mobility Domain Name
RF Group Name
User Idle Timeout (seconds)
300
ARP Timeout (seconds)
300
Web Radius Authentication
PAP
Operating Environment
Commercial (0 to 40 C)
Internal Temp Alarm Limits
0 to 65 C
WebAuth Proxy Redirection Mode
Disabled
WebAuth Proxy Redirection Port
0
Global IPv6 Config
Enabled
Web Color Theme
Default
HA SKU secondary unit
Disabled
Nas-Id
1. Multicast is not supported with FlexConnect on this platform.
Top


PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.0.0.7/frameInterfaceList.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Tunneling
IPv6
mDNS
Advanced
Interfaces
Entries 1 - 2 of 2
New...
Interface Name
VLAN Identifier
IP Address
Interface Type
Dynamic AP Management
IPv6 Address
management
untagged
10.0.0.7
Static
Enabled
::/128
virtual
N/A
192.0.2.1
Static
Not Supported
Top

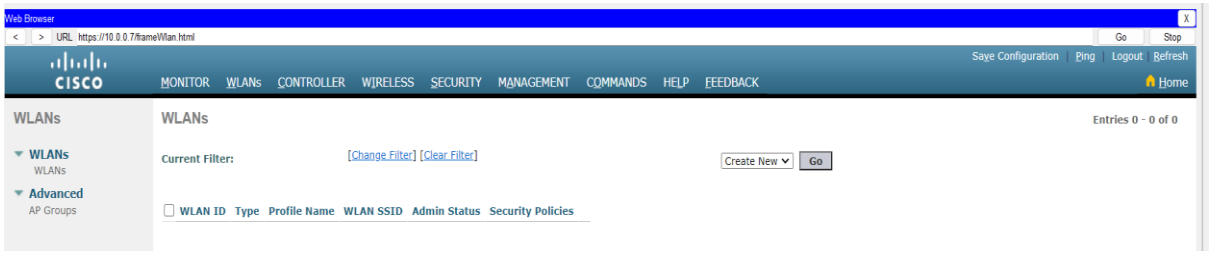

URL https://10.0.0.7/frameInterfaceCreate.html
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Interfaces > New
Interface Name
Wi-Fi
VLAN Id
40

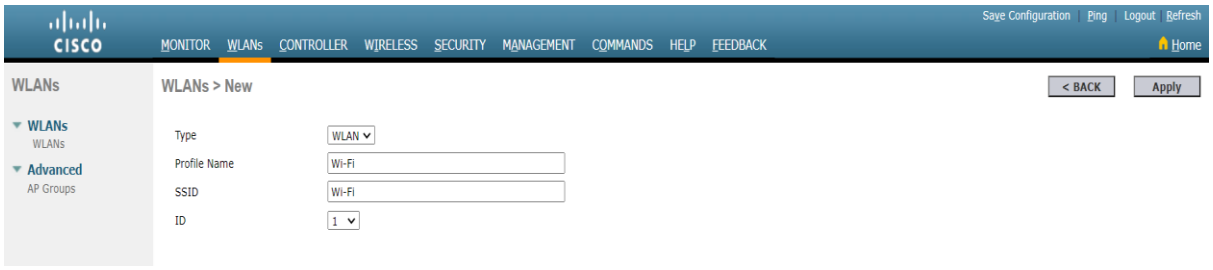

PC1
Physical Config Desktop Programming Attributes
Web Browser
URL https://10.0.0.7/frameInterfaceEdit.html
Go Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
Controller
Interfaces > Edit
< BACK Apply
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Tunneling
IPv6
mDNS
Advanced
General Information
Interface Name Wi-Fi
MAC Address 00:01:96:E8:52:41
Configuration
Guest Lan
Quarantine
Quarantine Vlan Id 0
NAS-ID
Physical Information
Port Number 1
Backup Port 0
Active Port 0
Enable Dynamic AP Management
Interface Address
VLAN Identifier 40
IP Address 10.6.0.4
Netmask 255.255.255.0
Gateway 10.6.0.1
DHCP Information
Primary DHCP Server 10.0.0.76
Top

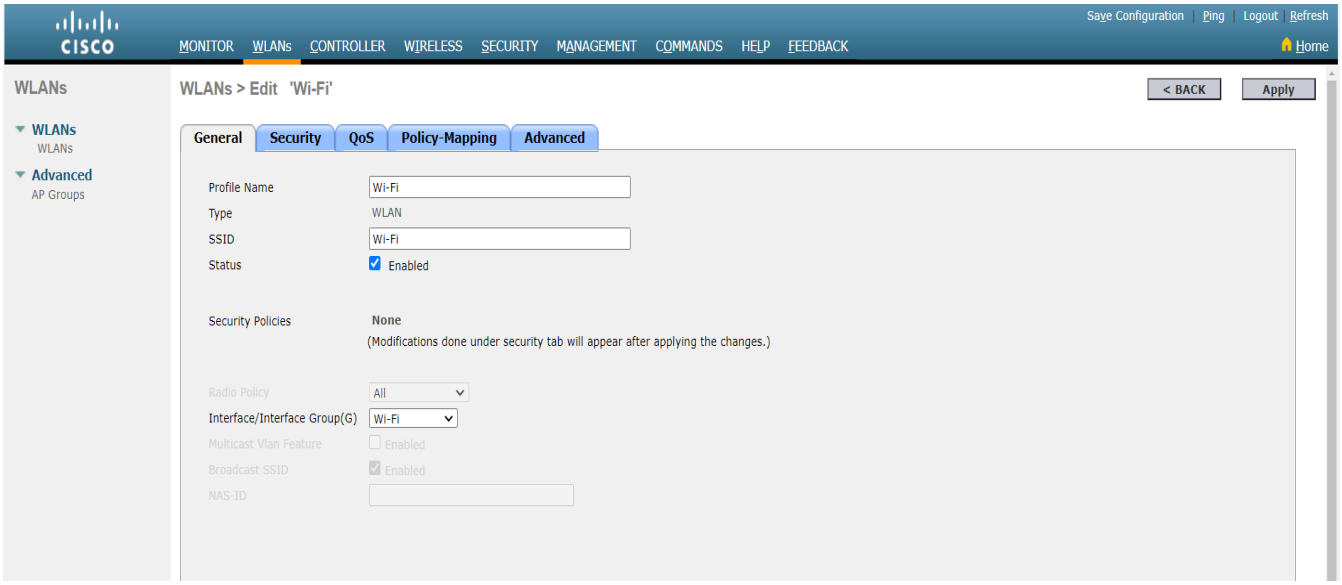

Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
Controller
Interfaces
Entries 1 - 3 of 3
New...
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Interface Name VLAN Identifier IP Address Interface Type Dynamic AP Management IPv6 Address
Wi-Fi 40 10.6.0.4 Dynamic Disabled Remove
management untagged 10.0.0.7 Static Enabled ::/128
virtual N/A 192.0.2.1 Static Not Supported

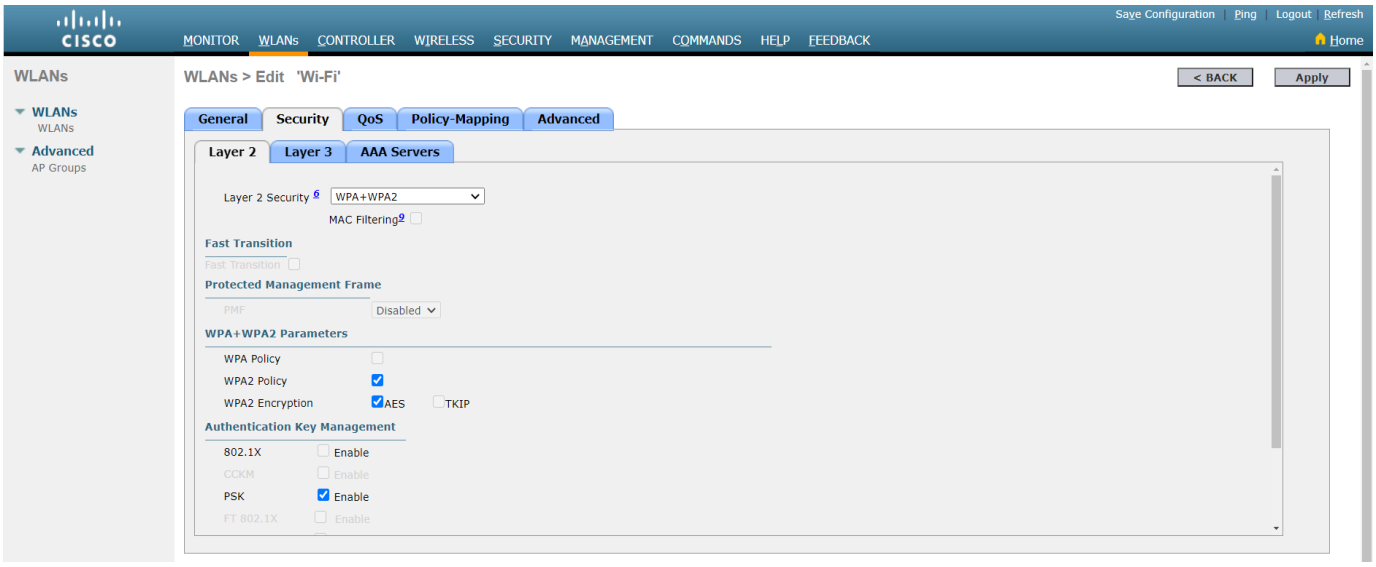
9.3 WLAN Configuration:

- Profile Name: Wi-Fi
- SSID: Wi-Fi
- WLAN ID: 1
- Status: Enabled
- Security: WPA2-PSK with AES encryption
- Pre-shared Key: cisco123




Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
Advanced
AP Groups
WLANs > Edit 'Wi-Fi'
< BACK
Apply
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
Wi-Fi
Type
WLAN
SSID
Wi-Fi
Status
Enabled
Security Policies
None
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G)
Wi-Fi
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
Advanced
AP Groups
WLANs > Edit 'Wi-Fi'
< BACK
Apply
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Authentication Key Management
802.1X
Enable
CCKM
Enable
PSK
Enable
FT 802.1X
Enable


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
Advanced
AP Groups
WLANs
Entries 1 - 1 of 1
Current Filter:
[Change Filter] [Clear Filter]
Create New
Go
WLAN ID
Type
Profile Name
WLAN SSID
Admin Status
Security Policies
1
WLAN
Wi-Fi
Wi-Fi
Enabled
[WPA2][Auth(PSK)]
Remove

**Conclusion**

This enterprise network successfully implements all specified requirements including:

- Redundant hierarchical design
- VLAN segmentation and trunking
- Gateway redundancy with HSRP
- Dynamic routing with OSPF
- Comprehensive security features
- Multiple network services (DHCP, DNS, NTP, etc.)
- Dual ISP connectivity with failover
- Wireless network integration
- IPv6 readiness

The network is production-ready with proper security, redundancy, and manageability considerations. All configurations follow Cisco best practices and the provided specifications exactly.