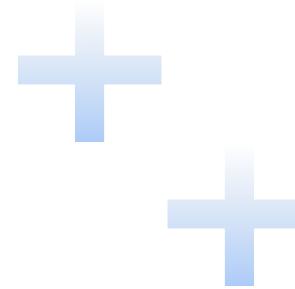


Network Design and Implementation for Corporate Headquarters

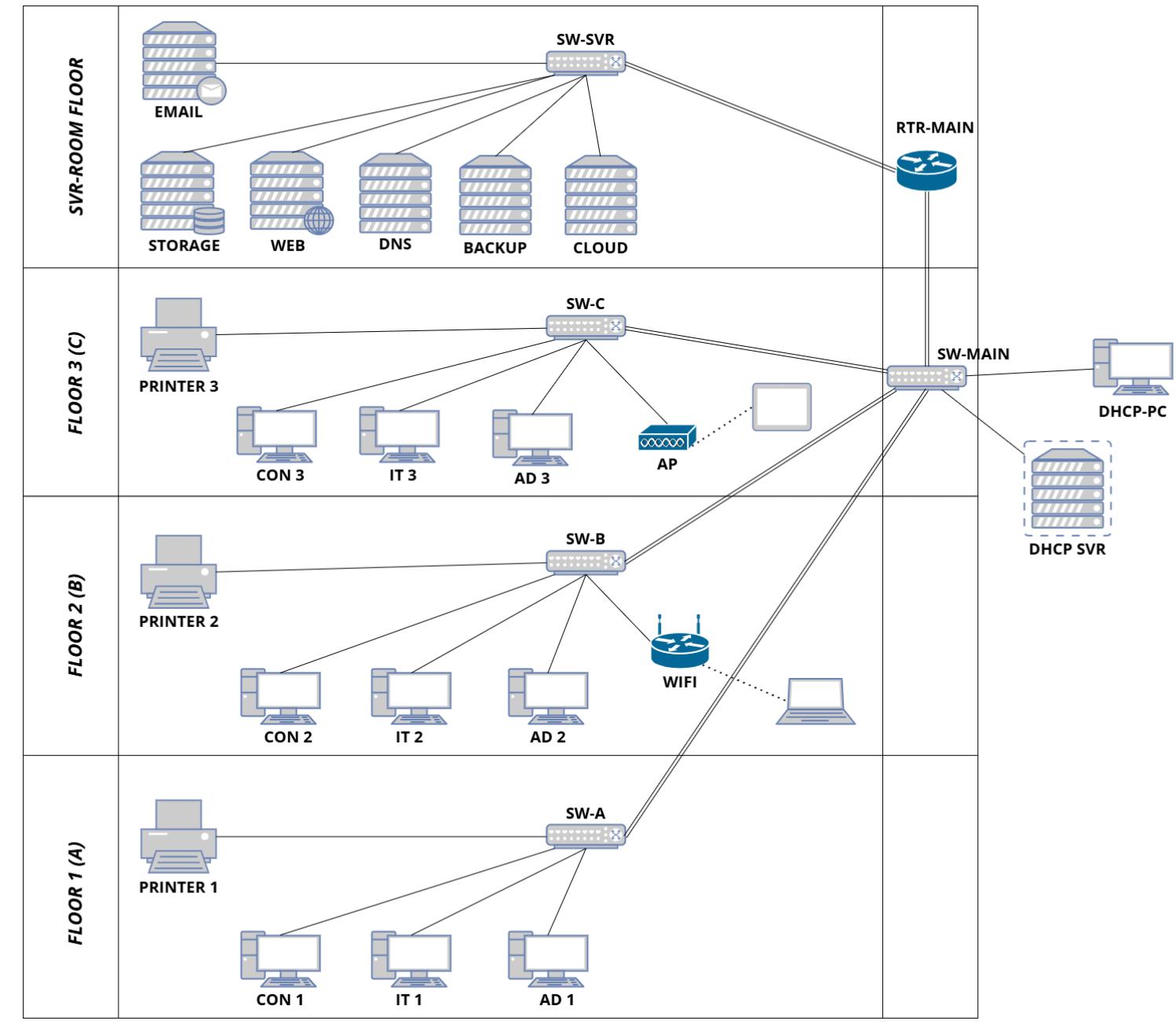
By Anjula Meegalla



Project Aim

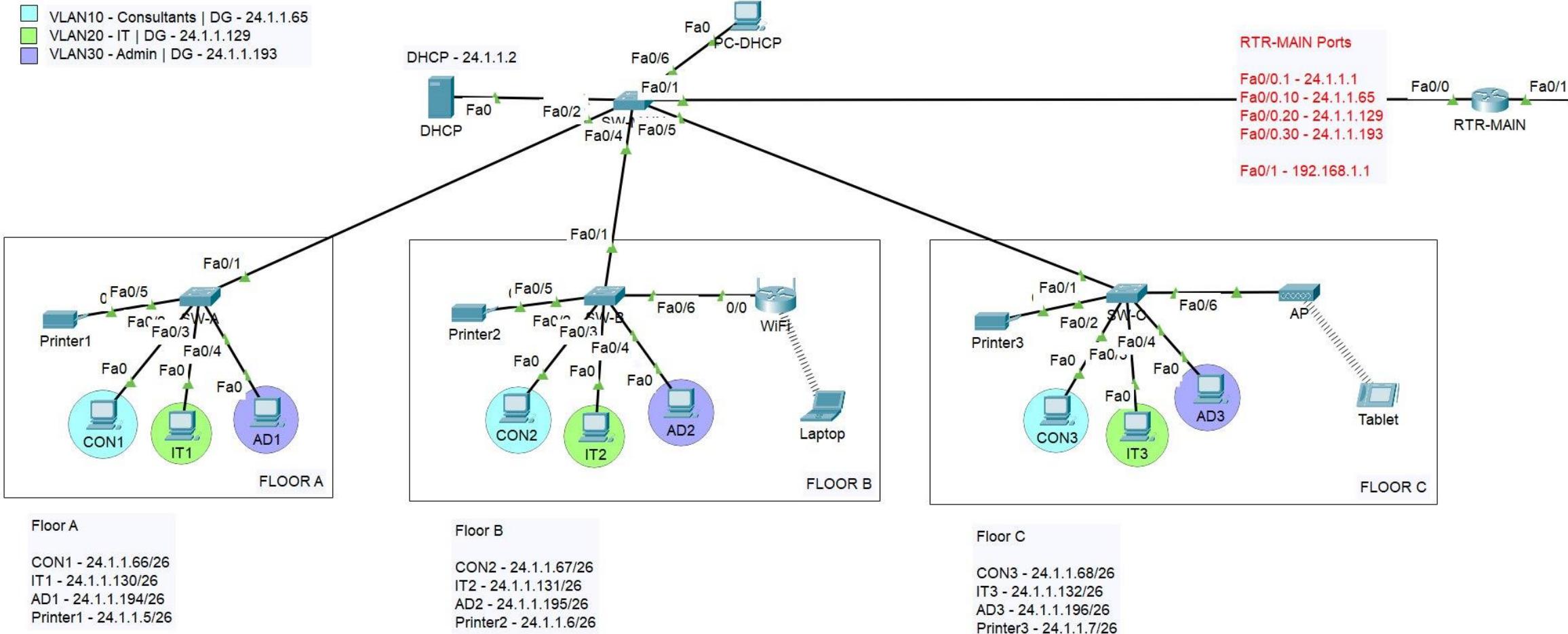
To apply core networking principles to design and simulate a secure, scalable, and multi-VLAN network that meets a given business specification.

3

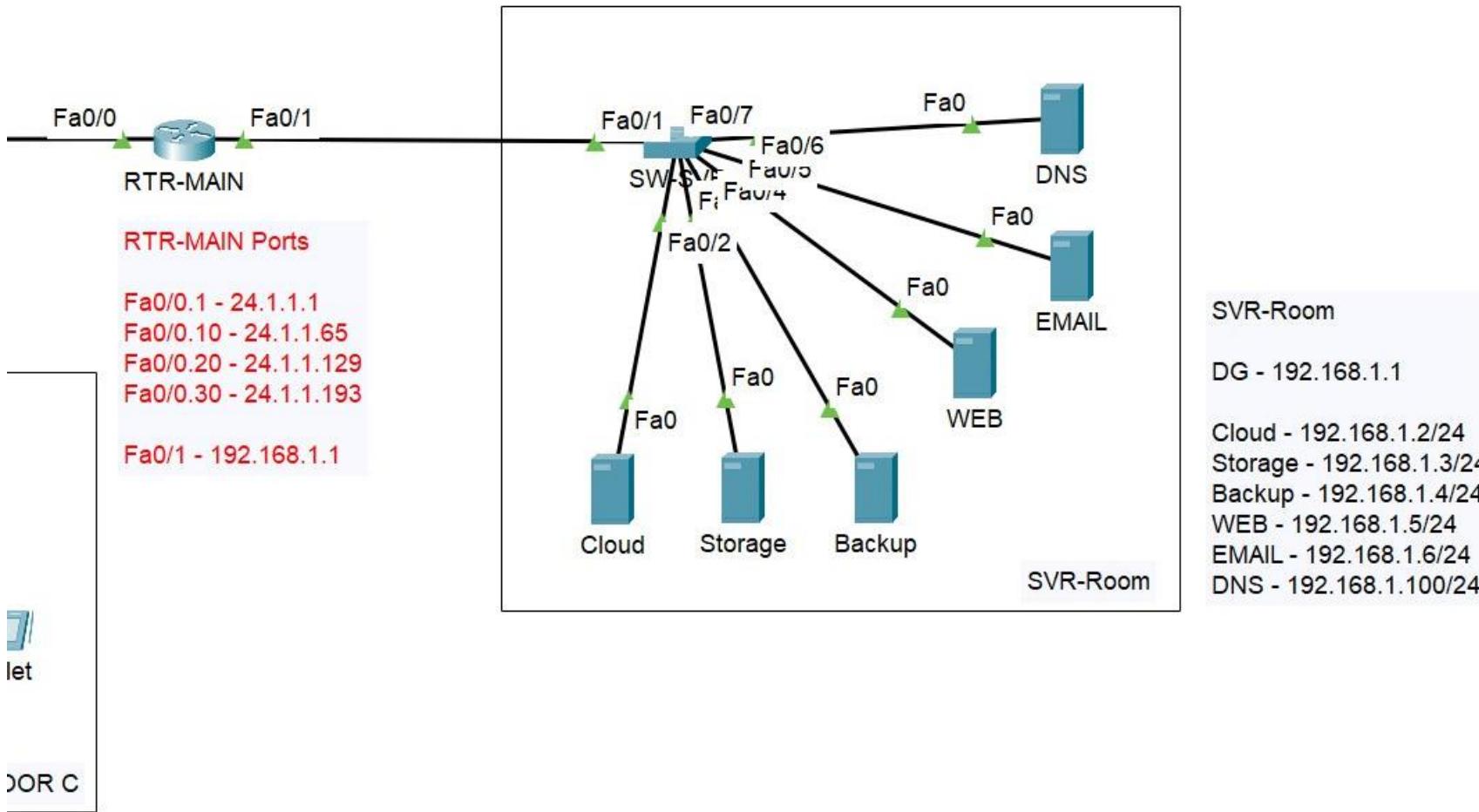


Network Diagram

Packet Tracer Simulation



Packet Tracer Simulation



Implementation - Core Infrastructure

The screenshot shows the configuration of a Cisco switch named 'SW-A'. The configuration includes setting the password encryption, defining VLANs 10, 20, and 30, and configuring FastEthernet ports 0/1 through 0/6 as access ports. The configuration is highlighted in a green box.

```
no service password-encryption
!
hostname SW-A
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/3
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/4
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
```

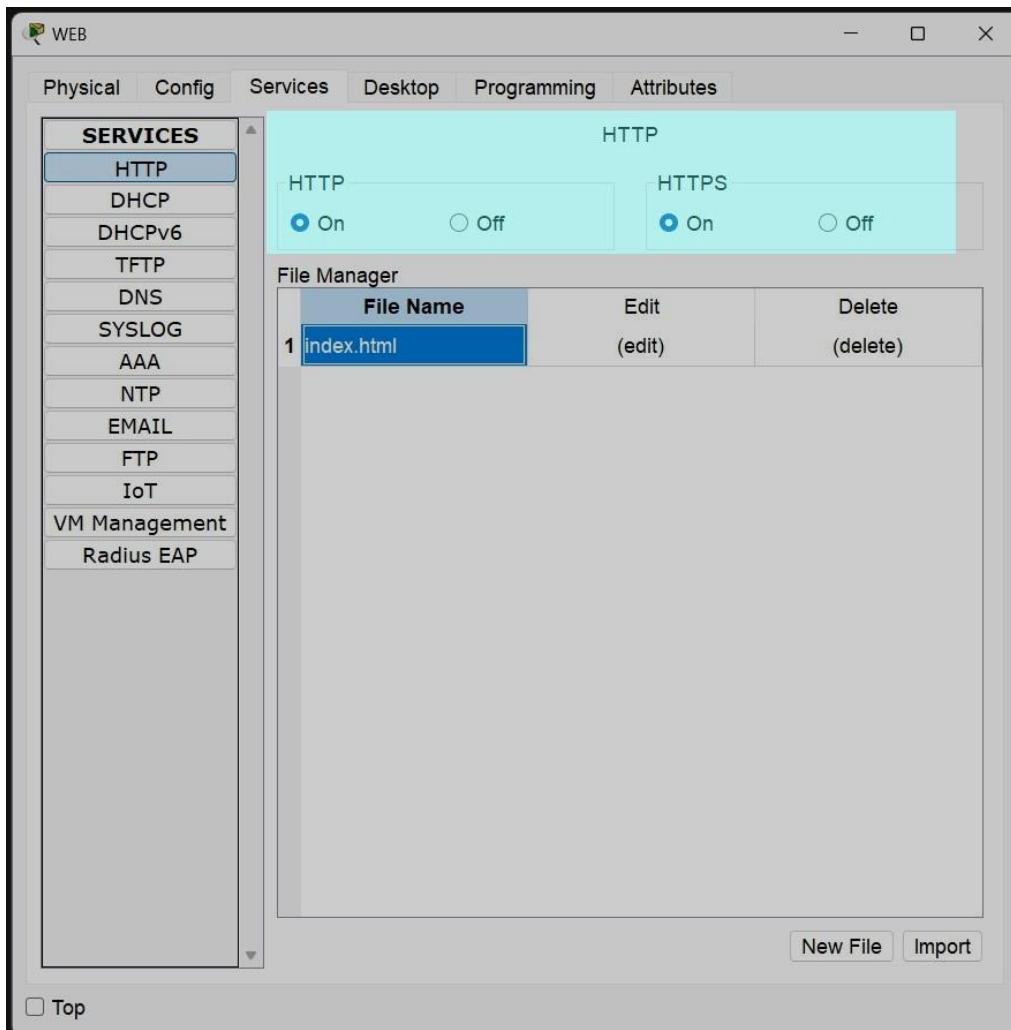
SW-A Configuration

The screenshot shows the configuration of a Cisco router named 'RTR-MAIN'. It includes the configuration of FastEthernet ports 0/0 to 0/30 and a Vlan1 interface. The configuration for ports 0/0 to 0/10 is highlighted in a green box.

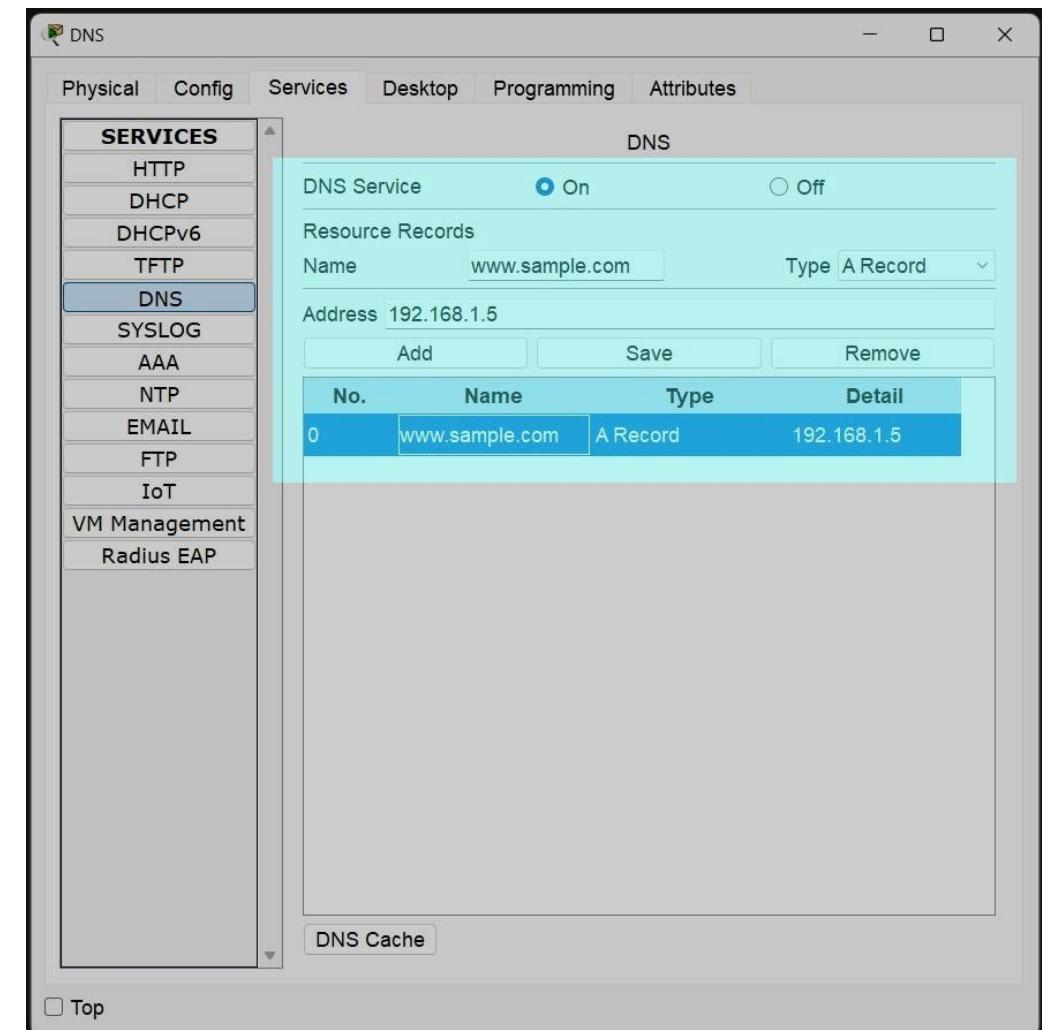
```
!
!
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet0/0.1
  encapsulation dot1Q 1 native
  ip address 24.1.1.1 255.255.255.192
!
interface FastEthernet0/0.10
  encapsulation dot1Q 10
  ip address 24.1.1.65 255.255.255.192
!
interface FastEthernet0/0.20
  encapsulation dot1Q 20
  ip address 24.1.1.129 255.255.255.192
!
interface FastEthernet0/0.30
  encapsulation dot1Q 30
  ip address 24.1.1.193 255.255.255.192
!
interface FastEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface Vlan1
--More-- |
```

RTR-MAIN Configuration

Implementation - Network Services

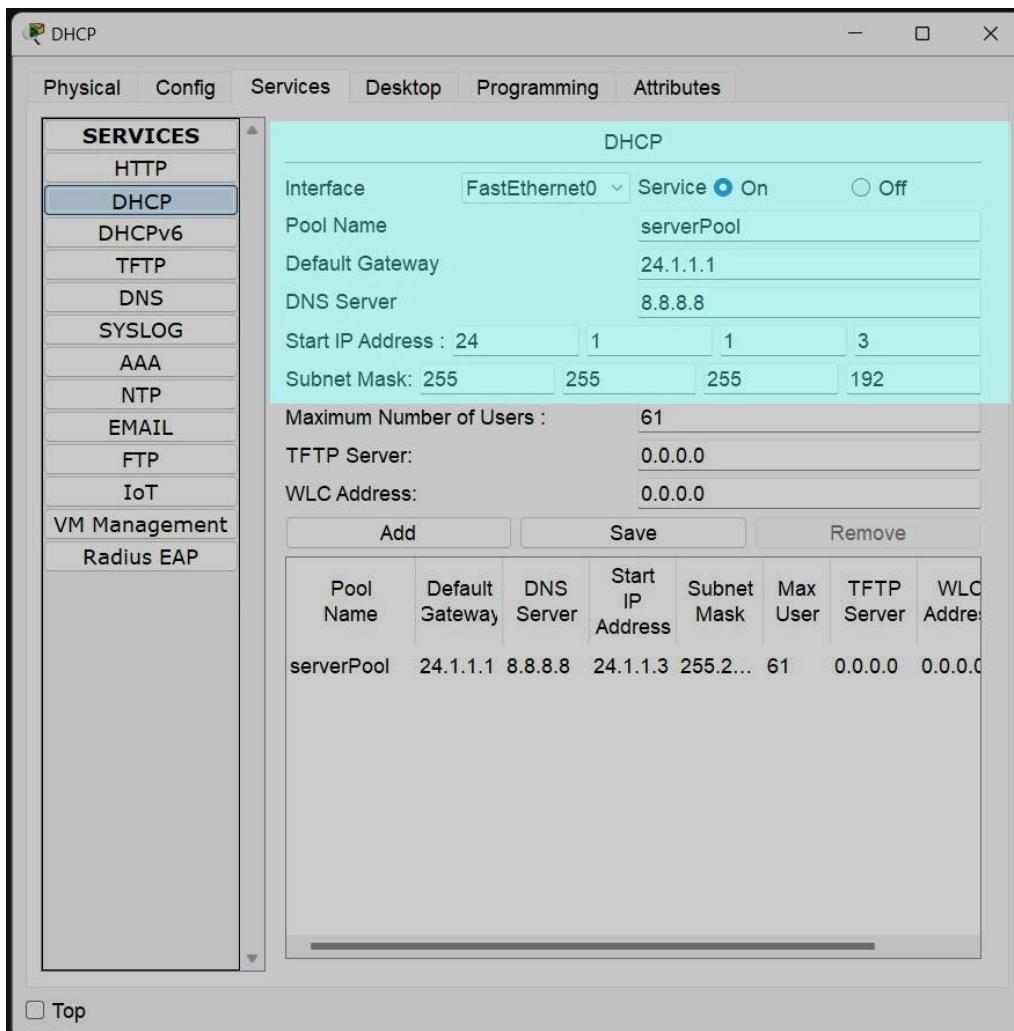


WEB SVR Configuration

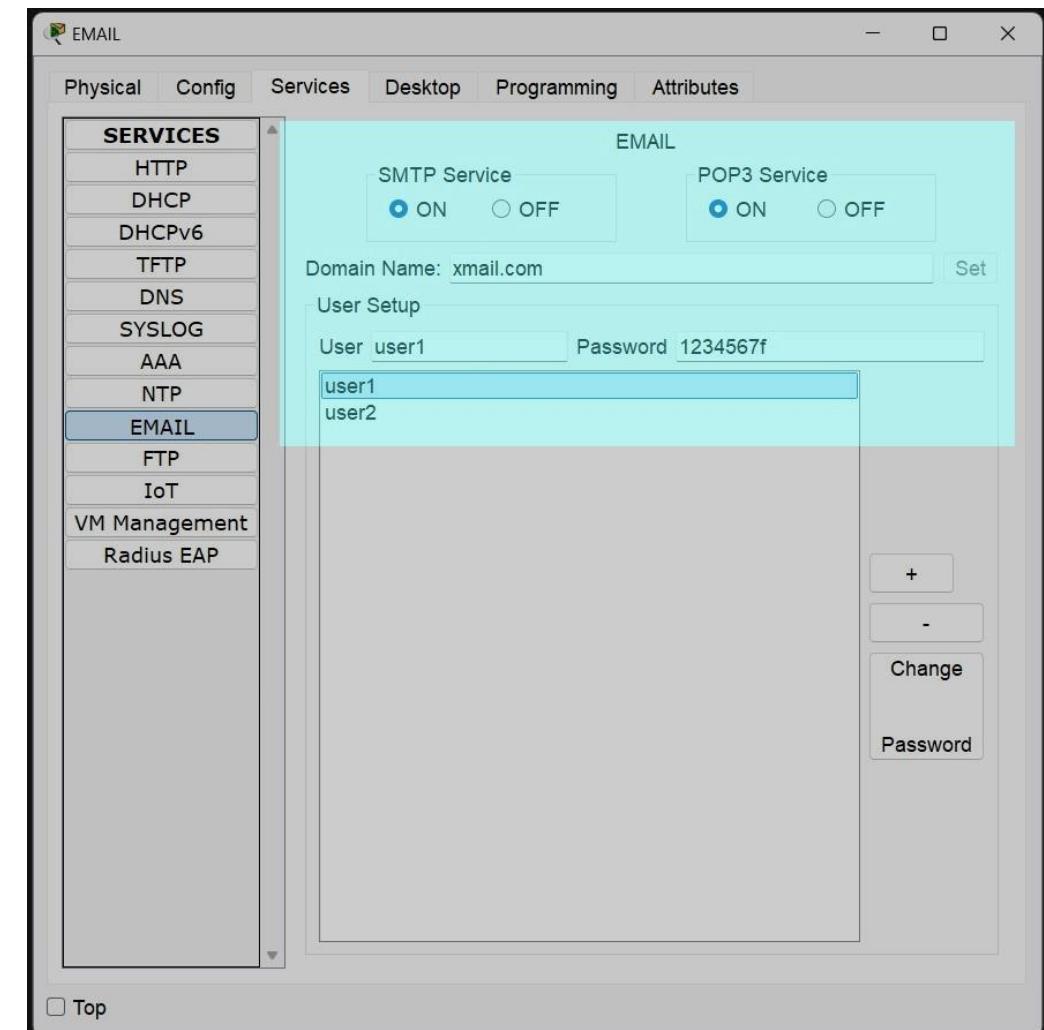


DNS SVR Configuration

Implementation - Network Services



DHCP SVR Configuration



EMAIL SVR Configuration

Test Results (Network Connectivity)

Cisco Packet Tracer PC Command Line 1.0
C:>ping 24.1.1.195

Pinging 24.1.1.195 with 32 bytes of data:

Request timed out.
Reply from 24.1.1.195: bytes=32 time=1ms TTL=127
Reply from 24.1.1.195: bytes=32 time<1ms TTL=127
Reply from 24.1.1.195: bytes=32 time=2ms TTL=127

Ping statistics for 24.1.1.195:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:>ping 24.1.1.195

Pinging 24.1.1.195 with 32 bytes of data:

Reply from 24.1.1.195: bytes=32 time=2ms TTL=127
Reply from 24.1.1.195: bytes=32 time<1ms TTL=127
Reply from 24.1.1.195: bytes=32 time<1ms TTL=127
Reply from 24.1.1.195: bytes=32 time<1ms TTL=127

Ping statistics for 24.1.1.195:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:>

“ping” Command Test

Cisco Packet Tracer PC Command Line 1.0
C:>tracert 192.168.1.100

Tracing route to 192.168.1.100 over a maximum of 30 hops:

1 1 ms 0 ms 0 ms 24.1.1.129
2 * 0 ms 0 ms 192.168.1.100

Trace complete.

C:>tracert 24.1.1.196

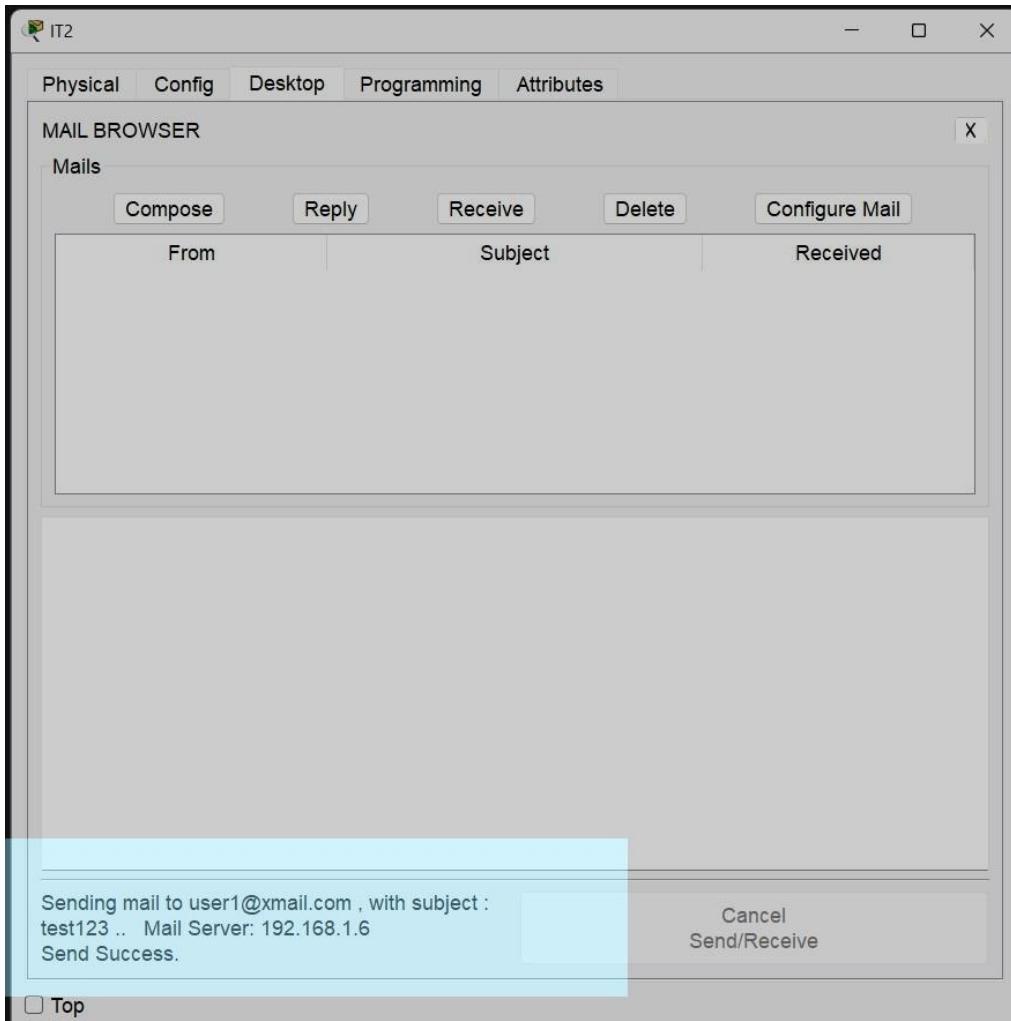
Tracing route to 24.1.1.196 over a maximum of 30 hops:

1 0 ms 1 ms 0 ms 24.1.1.129
2 * 0 ms 0 ms 24.1.1.196

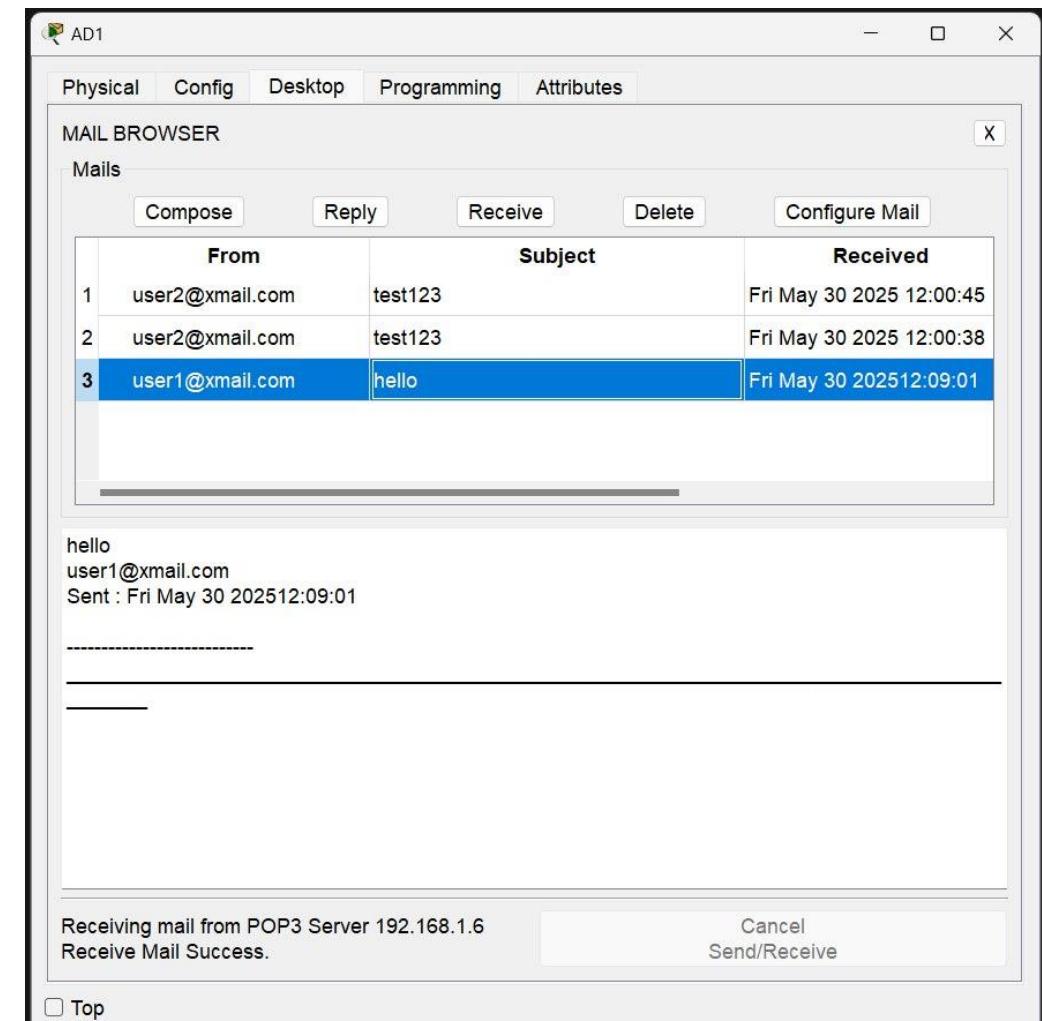
Trace complete.

“tracert” Command Test

Test Results (Email Send/Receive)

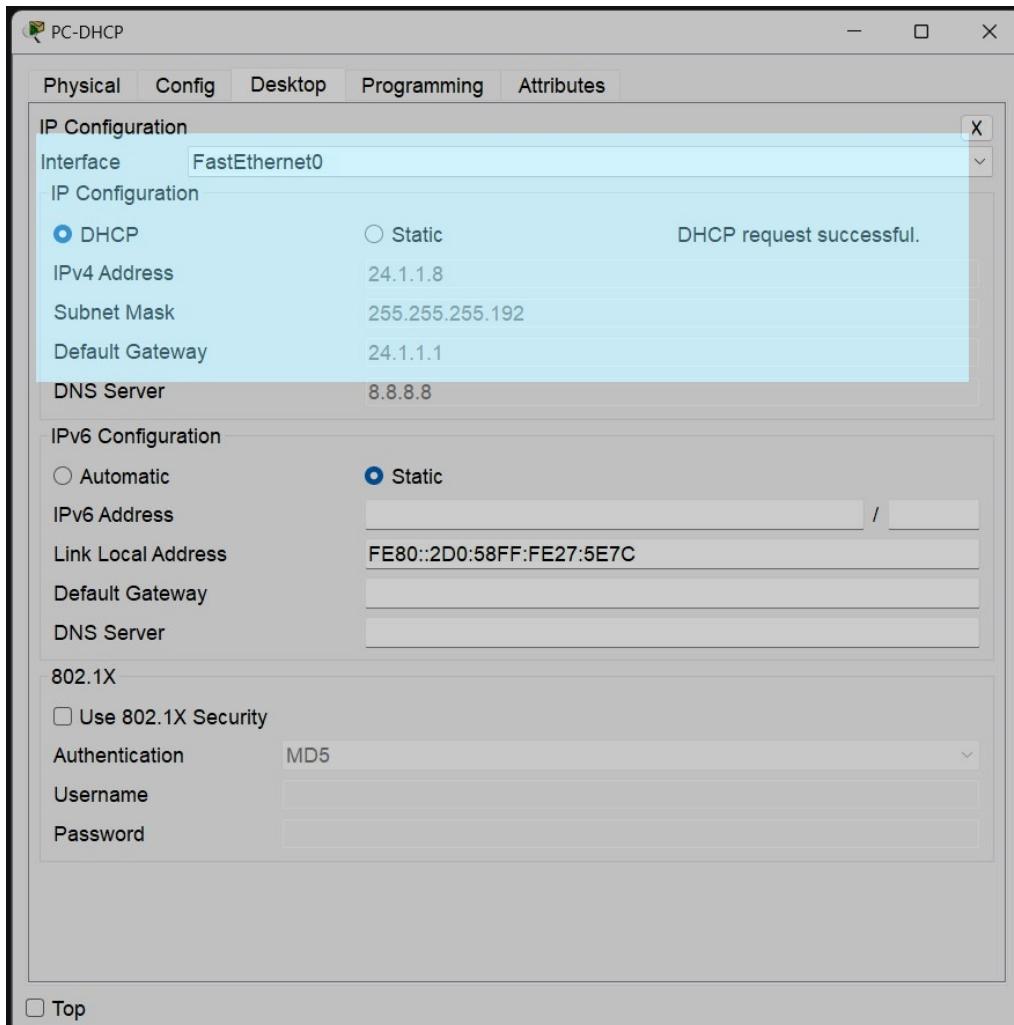


EMAIL Send Test



EMAIL Receive Test

Test Results



DHCP IP Test

```
C:\>nslookup www.sample.com
Server: [192.168.1.100]
Address: 192.168.1.100

Non-authoritative answer:
Name: www.sample.com
Address: 192.168.1.5

C:\>
```

```
CON3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>nslookup www.sample.com
Server: [192.168.1.100]
Address: 192.168.1.100

Non-authoritative answer:
Name: www.sample.com
Address: 192.168.1.5

C:\>
```

CON3

Physical Config Desktop Programming Attributes

Web Browser

< > URL <http://www.sample.com> Go Stop

A SAMPLE WEB PAGE

DNS Test

Live Demo - Network Verification

1. Inter-VLAN Connectivity
Test (ping)
2. Routing Path Verification
(traceroute)
3. DNS & Web Service Test
4. Email Function Test
5. DHCP Test



Analysis of Test Gaps

1. Wireless Coverage



Gap - While basic connection tests were successful, a minor gap was noted from user feedback, which suggested potential weak signal strength in the corner areas of Floor B.

2. Network Scalability

Gap - The network was verified under normal simulated conditions but has not been stress-tested to confirm its performance under peak load from all 50 employees, representing a future scalability risk.



Analysis of Test Gaps

3. Advanced Security



Gap - The implemented security measures are foundational. A comprehensive audit for advanced threats and vulnerabilities has not yet been performed, which is a necessary step for an organization handling sensitive data.

Summary of Gaps

- The core wired network and services are fully functional.
- Identified gaps relate primarily to future-proofing; wireless optimization, proving scalability, and advanced security hardening.



Further Improvements (Performance & Resilience)



To Improve Wireless Performance:

- Conduct a professional site survey to map RF coverage.
- Plan a future upgrade to Wi-Fi 6 access points.
- Deploy a Wireless LAN Controller (WLC) for centralized management.

To Improve Scalability & Resilience:

- Implement Layer 3 switching to accelerate inter-VLAN routing.
- Use Link Aggregation (EtherChannel) to increase bandwidth and redundancy.
- Deploy a second router for Gateway Redundancy.



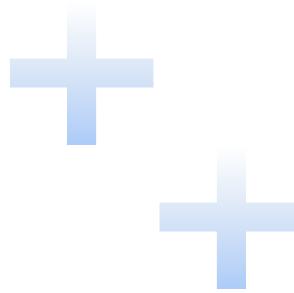
Further Improvements (Security)



To Strengthen Security Posture:

- Implement Network Access Control (NAC) to enforce security compliance on connecting devices.
- Deploy an Intrusion Detection/Prevention System (IDS/IPS) for real-time threat monitoring and blocking.
- Create more granular network segmentation for sensitive departments.
- Integrate automated vulnerability scanning with the patch management process.





Conclusion

Thank you

