Digital Egypt Pioneers Initiative (DEPI)

Cisco Cyber Security Engineer

Final Project Documentation

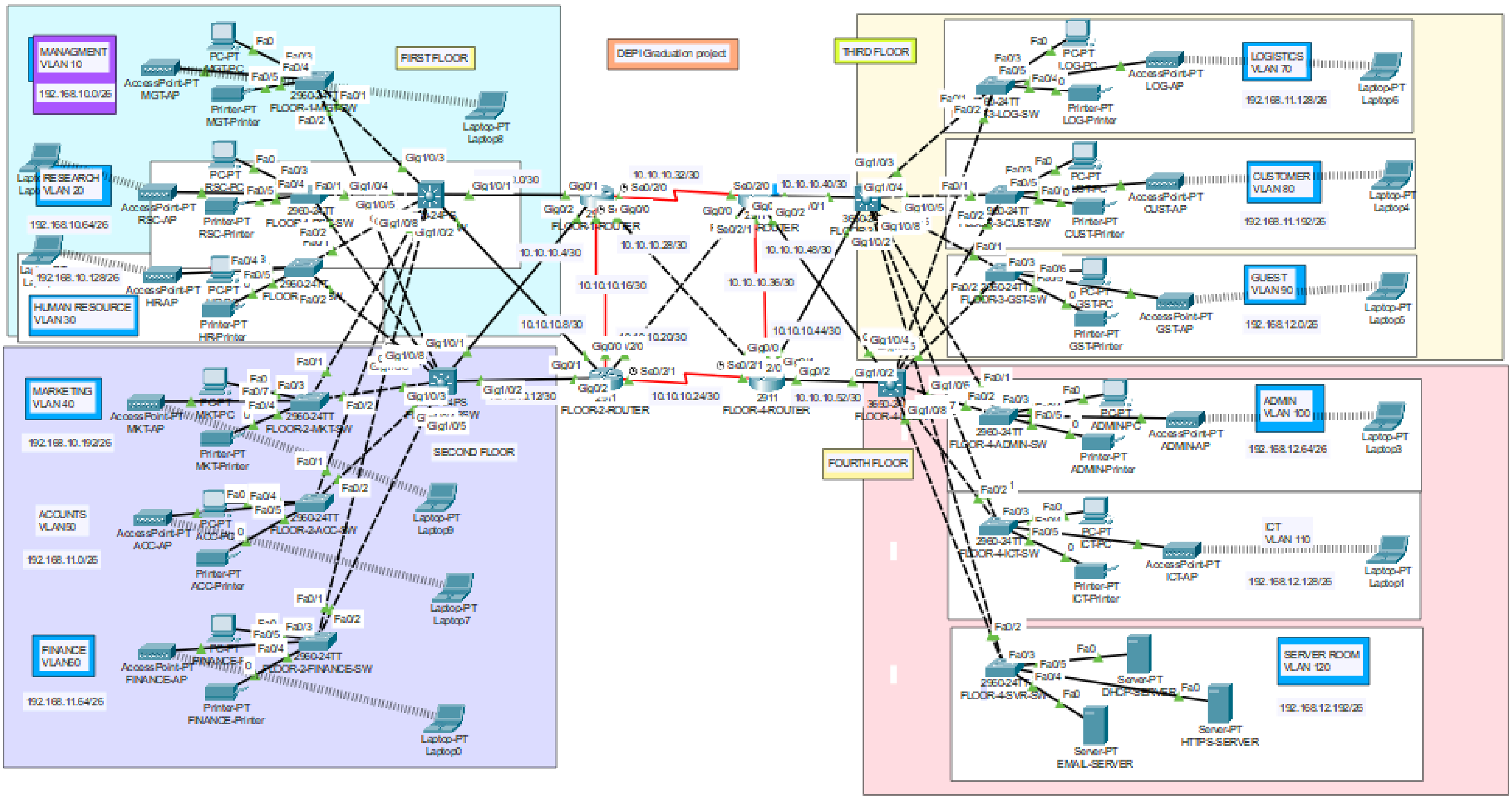
Bank Network Infrastructure Design & Implementation

Contents:

1- Project Overview

The network design project aims to create a reliable, scalable, and secure network infrastructure for a multi-story bank building. The network supports various departments across four floors, each with its own set of services and devices. The design incorporates high availability, efficient traffic management, and secure access for both wired and wireless devices.

Network Topology Diagram



2- Network Topology Overview

2.1 Physical Layout

- The bank’s network spans four floors, each containing multiple departments with dedicated network equipment:
  - First Floor: Management, Research, Human Resources.
  - Second Floor: Marketing, Accounts, Finance.
  - Third Floor: Logistics, Customer Service, Guest Area.
  - Fourth Floor: Administration, IT, Server Room.
- The floors are connected using core routers configured in a mesh topology for redundancy.

2.2 Logical Layout

- VLANs are used to segment the network logically, enhancing security and performance.
- Inter-VLAN routing is configured on routers to enable communication between VLANs where necessary.
- Access Control Lists (ACLs) are applied to restrict traffic between departments and enforce security policies.

3- VLAN Configuration

Each department is assigned a separate VLAN to isolate traffic, control broadcast domains, and enhance security. The VLAN assignments are as follows:

Floor	Dept	VLAN ID	Subnet
First Floor	Management	10	192.168.10.0/26
	Research	20	192.168.10.64/26
	Human Resources	30	192.168.10.128/26
Second Floor	Marketing	40	192.168.10.192/26
	Accounts	50	192.168.11.0/26
	Finance	60	192.168.11.64/26
Third Floor	Logistics	70	192.168.11.128/26
	Customer Service	80	192.168.11.192/26
	Guest	90	192.168.12.0/26
Fourth Floor	Administration	100	192.168.12.64/26
	IT	110	192.168.12.128/26
	Server Room	120	192.168.12.192/26

4- Routing and Interconnectivity

4.1 Routers Configuration

- Four routers (FLOOR 1-ROUTER, FLOOR 2-ROUTER, FLOOR 3-ROUTER, and FLOOR 4-ROUTER) are deployed, with connections to each switch on their respective floors.
- Each router is configured with subinterfaces for each VLAN, enabling inter-VLAN routing.
- The IP addresses assigned to router interfaces serve as the default gateways for the devices within their respective VLANs.

4.2 Redundancy

- The routers are interconnected in a full mesh topology, providing multiple paths for traffic.
- Redundant links ensure continuous connectivity in case of a single link or device failure.
- The Spanning Tree Protocol (STP) is configured on switches to prevent network loops while allowing redundant paths.

5- Network Security

5.1 Access Control Lists (ACLs)

- ACLs are applied on routers to filter traffic based on source and destination IP addresses.
- The Guest VLAN has restricted access, only allowing traffic to the internet, while blocking access to sensitive internal resources.

5.2 Wireless Security

- Wireless networks are deployed on each floor using Access Points (APs) with multiple SSIDs corresponding to the VLANs.
- WPA2 encryption is used to secure the wireless network.
- Separate SSIDs for guest users provide isolated internet access, without allowing access to internal network resources.

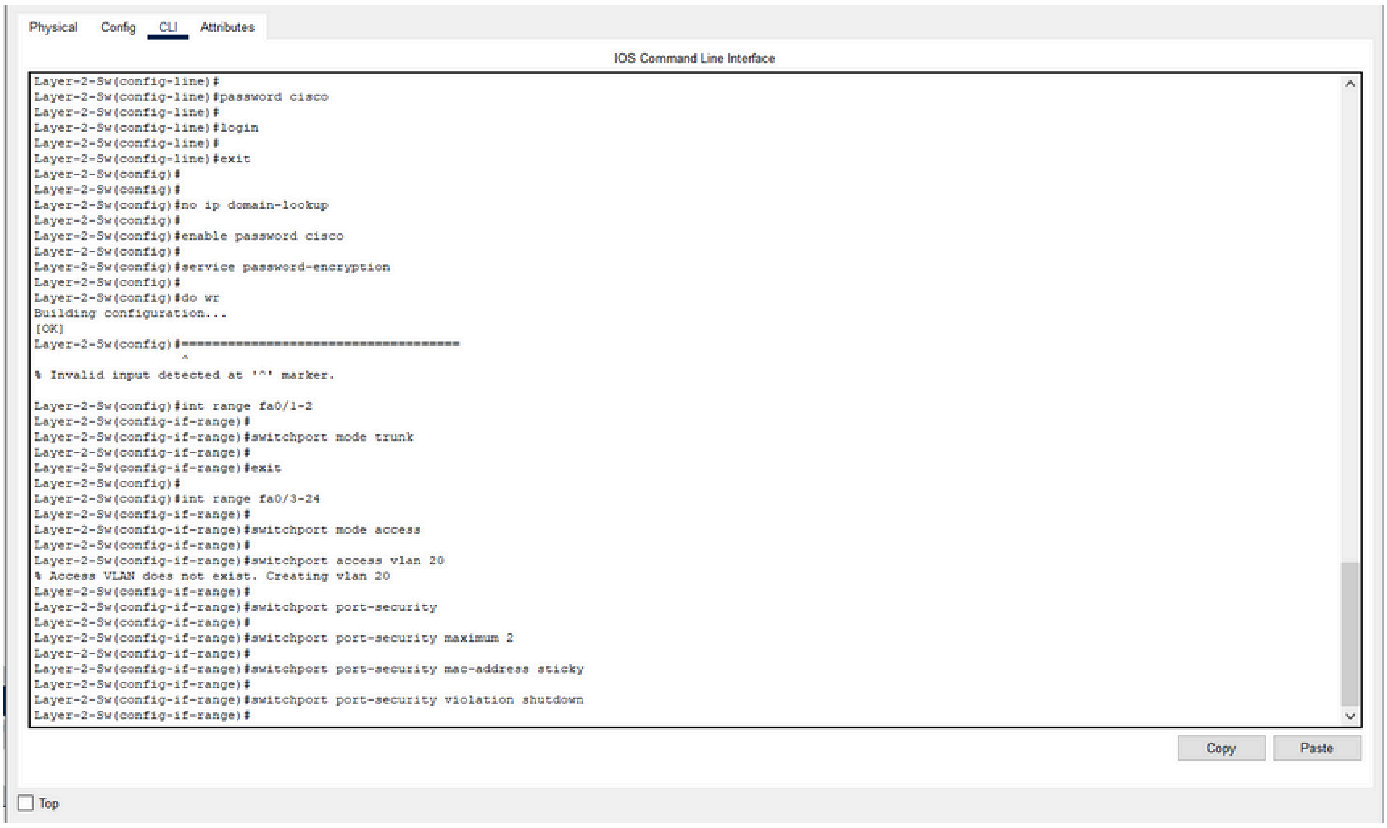
5.3 Network Segmentation

- The use of VLANs ensures segmentation, reducing the impact of broadcast traffic and isolating different departments.
- The server room VLAN is further isolated and protected using ACLs to limit access only to authorized personnel and services.

6- Devices Configuration

6.1 Switches

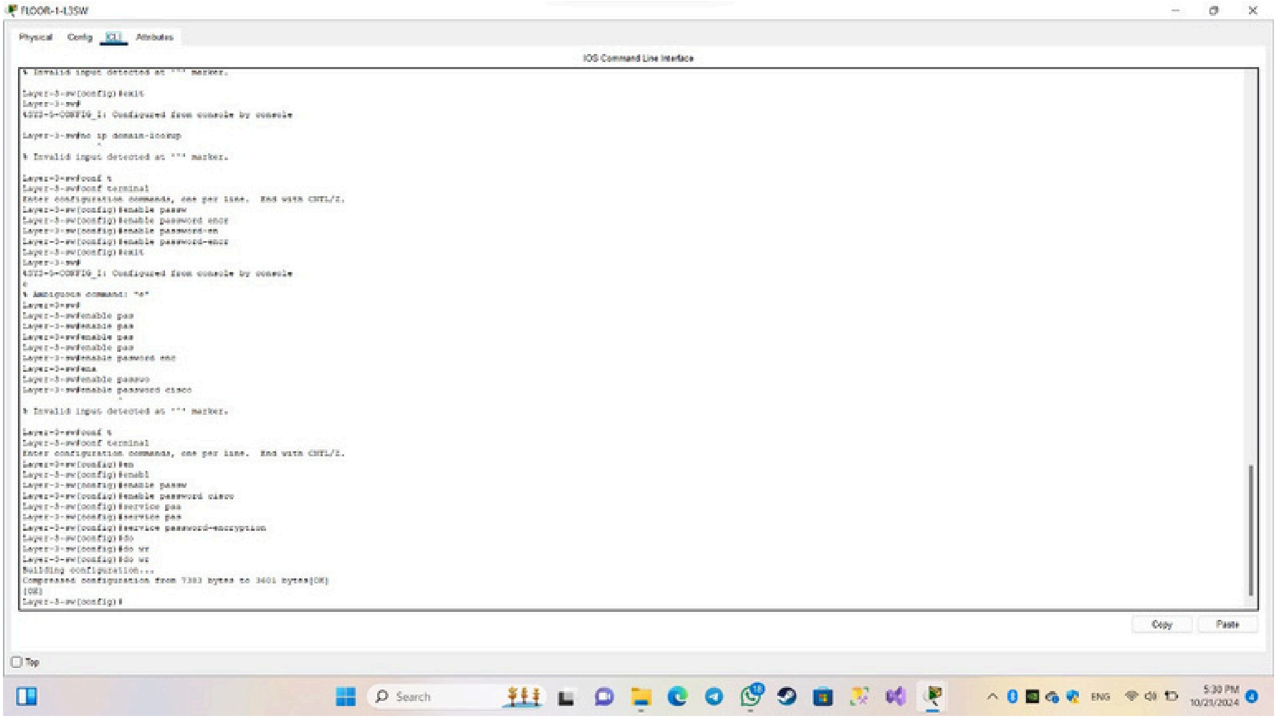
- Access Switches: Each floor has dedicated access switches for connecting end-user devices (PCs, printers, IP phones).
- Core Switches: The core switches aggregate connections from the access switches and uplink to the routers.



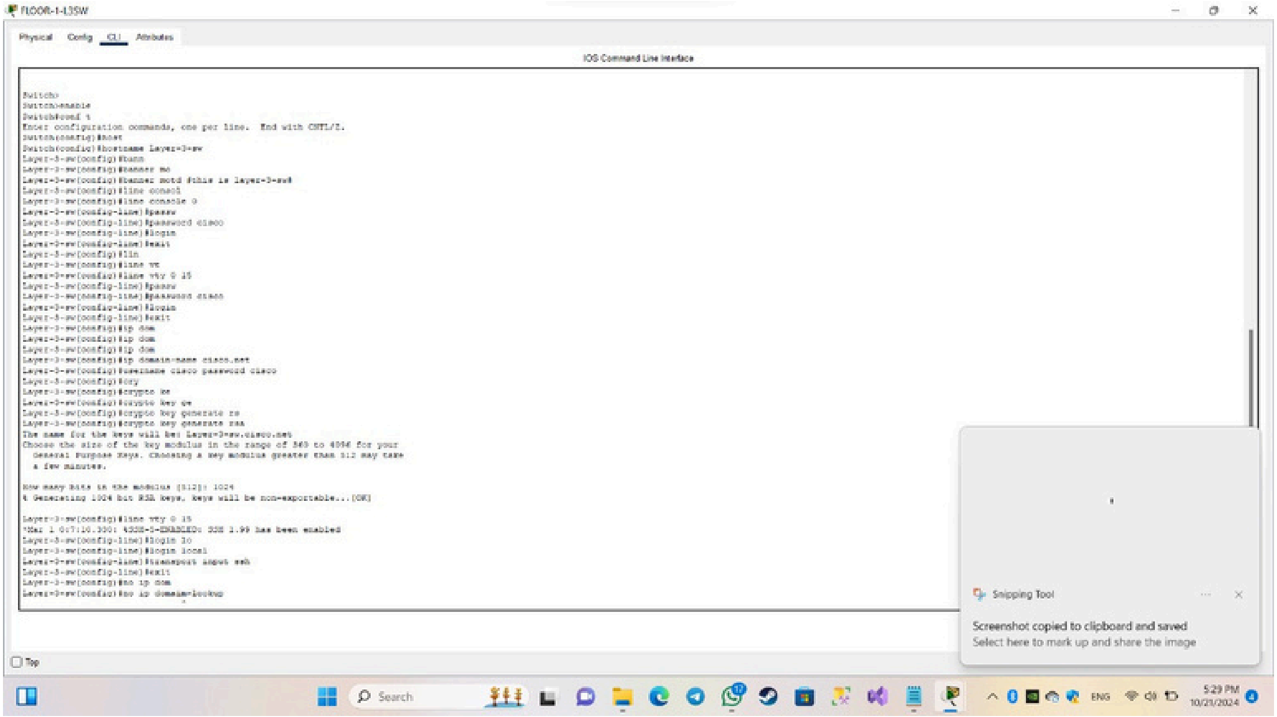
```
Layer-2-Sw(config-line)#
Layer-2-Sw(config-line)#password cisco
Layer-2-Sw(config-line)#
Layer-2-Sw(config-line)#login
Layer-2-Sw(config-line)#
Layer-2-Sw(config-line)#exit
Layer-2-Sw(config)#
Layer-2-Sw(config)#
Layer-2-Sw(config)#no ip domain-lookup
Layer-2-Sw(config)#
Layer-2-Sw(config)#enable password cisco
Layer-2-Sw(config)#
Layer-2-Sw(config)#service password-encryption
Layer-2-Sw(config)#
Layer-2-Sw(config)#do wr
Building configuration...
[OK]
Layer-2-Sw(config)#====================================
                   ^
% Invalid input detected at '^' marker.

Layer-2-Sw(config)#int range fa0/1-2
Layer-2-Sw(config-if-range)#
Layer-2-Sw(config-if-range)#switchport mode trunk
Layer-2-Sw(config-if-range)#
Layer-2-Sw(config-if-range)#exit
Layer-2-Sw(config)#
Layer-2-Sw(config)#int range fa0/3-24
Layer-2-Sw(config-if-range)#
Layer-2-Sw(config-if-range)#switchport mode access
Layer-2-Sw(config-if-range)#
Layer-2-Sw(config-if-range)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
Layer-2-Sw(config-if-range)#
Layer-2-Sw(config-if-range)#switchport port-security
Layer-2-Sw(config-if-range)#
Layer-2-Sw(config-if-range)#switchport port-security maximum 2
Layer-2-Sw(config-if-range)#
Layer-2-Sw(config-if-range)#switchport port-security mac-address sticky
Layer-2-Sw(config-if-range)#
Layer-2-Sw(config-if-range)#switchport port-security violation shutdown
Layer-2-Sw(config-if-range)#
```

Fig.1 Access Switches Configuration

6- Devices Configuration



```
% Invalid input detected at '^' marker.

Layer-3-sw(config)#exit
Layer-3-sw#
%SYS-5-CONFIG_I: Configured from console by console

Layer-3-sw#no ip domain-lookup
            ^
% Invalid input detected at '^' marker.

Layer-3-sw#conf t
Layer-3-sw#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Layer-3-sw(config)#enable passw
Layer-3-sw(config)#enable password encr
Layer-3-sw(config)#enable password-en
Layer-3-sw(config)#enable password-encr
Layer-3-sw(config)#exit
Layer-3-sw#
%SYS-5-CONFIG_I: Configured from console by console
e
% Ambiguous command: "e"
Layer-3-sw#
Layer-3-sw#enable pas
Layer-3-sw#enable pas
Layer-3-sw#enable pas
Layer-3-sw#enable pas
Layer-3-sw#enable pasword enc
Layer-3-sw#ena
Layer-3-sw#enable passwo
Layer-3-sw#enable password cisco
                   ^
% Invalid input detected at '^' marker.

Layer-3-sw#conf t
Layer-3-sw#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Layer-3-sw(config)#en
Layer-3-sw(config)#enabl
Layer-3-sw(config)#enable passw
Layer-3-sw(config)#enable password cisco
Layer-3-sw(config)#service pas
Layer-3-sw(config)#service pas
Layer-3-sw(config)#service password-encryption
Layer-3-sw(config)#do
Layer-3-sw(config)#do wr
Layer-3-sw(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3401 bytes[OK]
[OK]
Layer-3-sw(config)#
```



```
Switch>
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host
Switch(config)#hostname Layer-3-sw
Layer-3-sw(config)#bann
Layer-3-sw(config)#banner mo
Layer-3-sw(config)#banner motd #this is layer-3-sw#
Layer-3-sw(config)#line consol
Layer-3-sw(config)#line console 0
Layer-3-sw(config-line)#passw
Layer-3-sw(config-line)#password cisco
Layer-3-sw(config-line)#login
Layer-3-sw(config-line)#exit
Layer-3-sw(config)#lin
Layer-3-sw(config)#line vt
Layer-3-sw(config)#line vty 0 15
Layer-3-sw(config-line)#passw
Layer-3-sw(config-line)#password cisco
Layer-3-sw(config-line)#login
Layer-3-sw(config-line)#exit
Layer-3-sw(config)#ip dom
Layer-3-sw(config)#ip dom
Layer-3-sw(config)#ip dom
Layer-3-sw(config)#ip domain-name cisco.net
Layer-3-sw(config)#username cisco password cisco
Layer-3-sw(config)#cry
Layer-3-sw(config)#crypto ke
Layer-3-sw(config)#crypto key ge
Layer-3-sw(config)#crypto key generate rs
Layer-3-sw(config)#crypto key generate rsa
The name for the keys will be: Layer-3-sw.cisco.net
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]

Layer-3-sw(config)#line vty 0 15
*Mar 1 0:7:10.300: %SSH-5-ENABLED: SSH 1.99 has been enabled
Layer-3-sw(config-line)#login lo
Layer-3-sw(config-line)#login local
Layer-3-sw(config-line)#transport input ssh
Layer-3-sw(config-line)#exit
Layer-3-sw(config)#no ip dom
Layer-3-sw(config)#no ip domain-lookup
                           ^
```

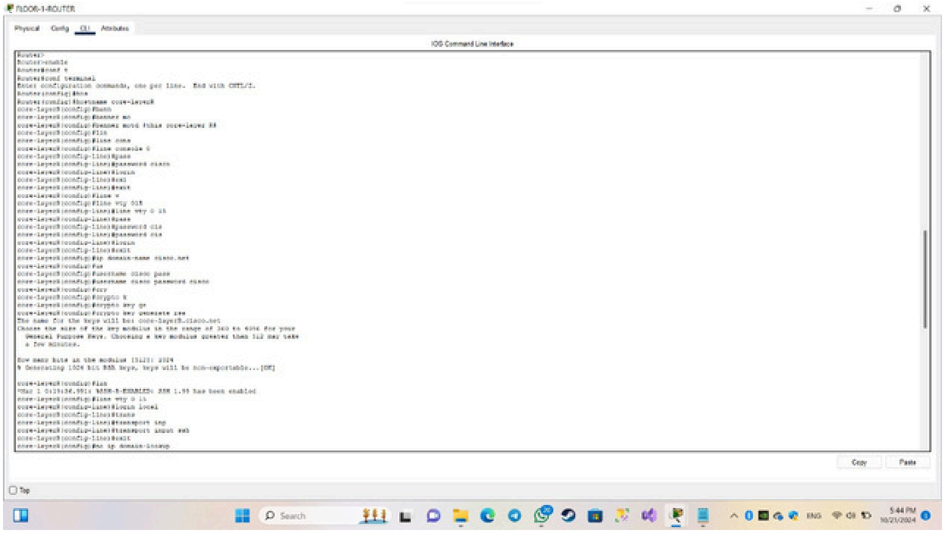
Screenshot copied to clipboard and saved
Select here to mark up and share the image

Fig.2 Core Switches Configuration

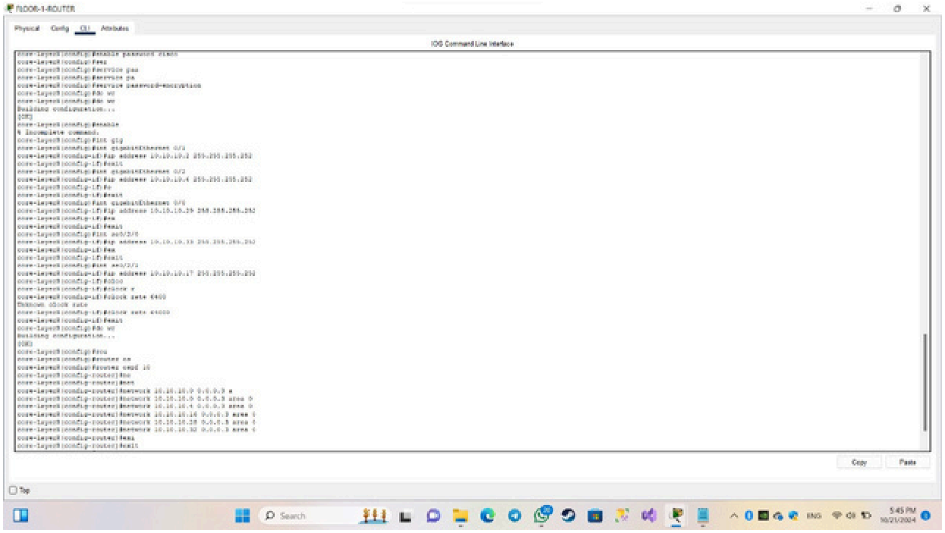
6- Devices Configuration

6.2 Routers

- FLOOR 1-ROUTER, FLOOR 2-ROUTER, FLOOR 3-ROUTER, FLOOR 4-ROUTER: Each router is configured with sub interfaces for VLANs and connected in a mesh topology for redundancy.
- Routing Protocol: Static routes are used for simplicity in this network, although future scalability may require a dynamic routing protocol like OSPF.



```
Router>
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ho
Router(config)#hostname core-layer3
core-layer3(config)#banm
core-layer3(config)#banner mo
core-layer3(config)#banner motd !this core-layer 3!
core-layer3(config)#li
core-layer3(config)#line cons
core-layer3(config)#line console 0
core-layer3(config-line)#pass
core-layer3(config-line)#password cisco
core-layer3(config-line)#login
core-layer3(config-line)#exi
core-layer3(config-line)#exit
core-layer3(config)#line v
core-layer3(config)#line vty 015
core-layer3(config-line)#line vty 0 15
core-layer3(config-line)#pass
core-layer3(config-line)#password cis
core-layer3(config-line)#password cis
core-layer3(config-line)#login
core-layer3(config-line)#exit
core-layer3(config)#ip domain-name cisco.net
core-layer3(config)#us
core-layer3(config)#username cisco pass
core-layer3(config)#username cisco password cisco
core-layer3(config)#cry
core-layer3(config)#crypto k
core-layer3(config)#crypto key ge
core-layer3(config)#crypto key generate rsa
The name for the keys will be: core-layer3.cisco.net
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]

core-layer3(config)#lin
*Mar 1 0:19:36.951: %SSH-5-ENABLED: SSH 1.99 has been enabled
core-layer3(config)#line vty 0 15
core-layer3(config-line)#login local
core-layer3(config-line)#trans
core-layer3(config-line)#transport inp
core-layer3(config-line)#transport input ssh
core-layer3(config-line)#exit
core-layer3(config)#no ip domain-lookup
```



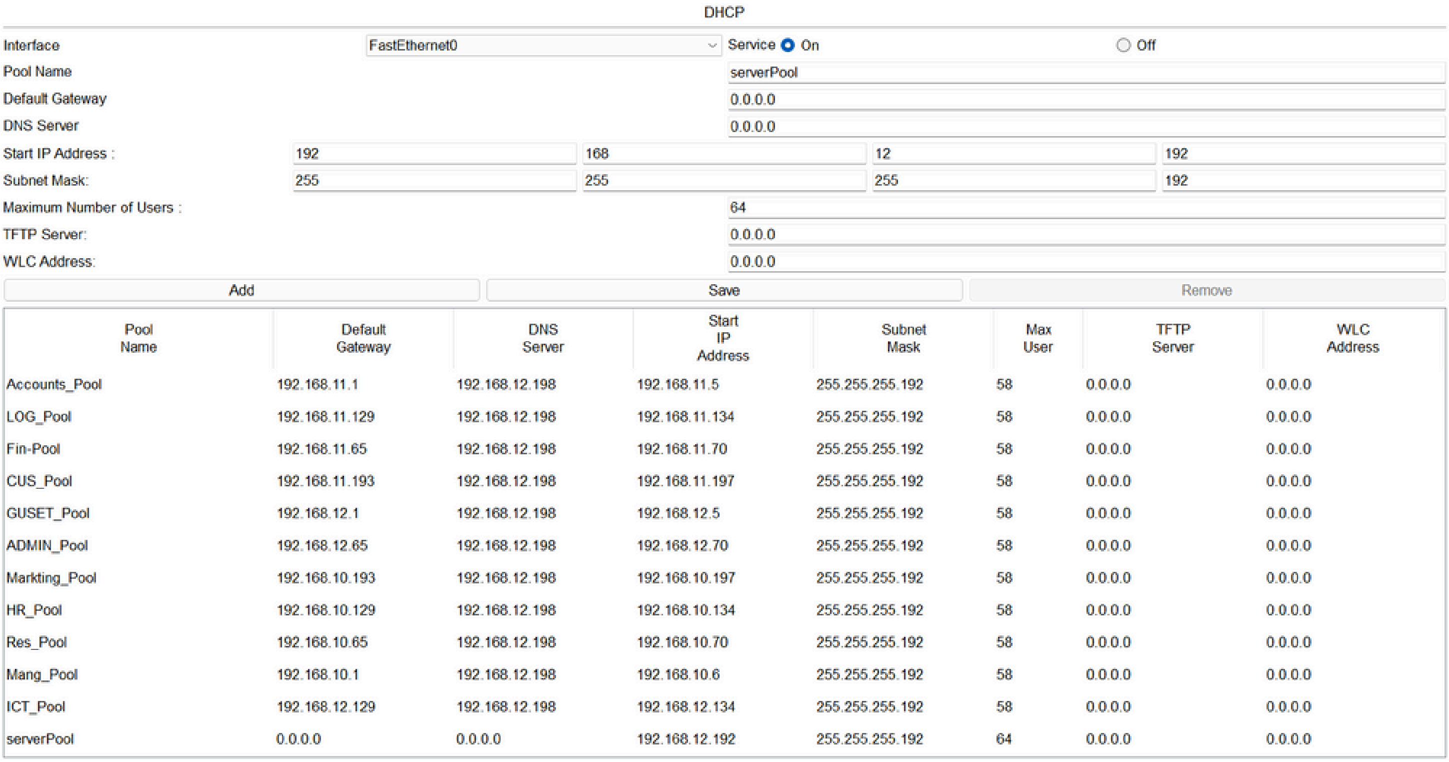
```
core-layer3(config)#enable password cisco
core-layer3(config)#ser
core-layer3(config)#service pas
core-layer3(config)#service pa
core-layer3(config)#service password-encryption
core-layer3(config)#do wr
core-layer3(config)#do wr
Building configuration...
[OK]
core-layer3(config)#enable
% Incomplete command.
core-layer3(config)#int gig
core-layer3(config)#int gigabitEthernet 0/1
core-layer3(config-if)#ip address 10.10.10.2 255.255.255.252
core-layer3(config-if)#exit
core-layer3(config)#int gigabitEthernet 0/2
core-layer3(config-if)#ip address 10.10.10.6 255.255.255.252
core-layer3(config-if)#no
core-layer3(config-if)#exit
core-layer3(config)#int gigabitEthernet 0/0
core-layer3(config-if)#ip address 10.10.10.29 255.255.255.252
core-layer3(config-if)#no
core-layer3(config-if)#exit
core-layer3(config)#int se0/2/0
core-layer3(config-if)#ip address 10.10.10.33 255.255.255.252
core-layer3(config-if)#no
core-layer3(config-if)#exit
core-layer3(config)#int se0/2/1
core-layer3(config-if)#ip address 10.10.10.17 255.255.255.252
core-layer3(config-if)#clo
core-layer3(config-if)#clock r
core-layer3(config-if)#clock rate 6400
Unknown clock rate
core-layer3(config-if)#clock rate 64000
core-layer3(config-if)#exit
core-layer3(config)#do wr
Building configuration...
[OK]
core-layer3(config)#rou
core-layer3(config)#router os
core-layer3(config)#router ospf 10
core-layer3(config-router)#ne
core-layer3(config-router)#net
core-layer3(config-router)#network 10.10.10.0 0.0.0.3 a
core-layer3(config-router)#network 10.10.10.0 0.0.0.3 area 0
core-layer3(config-router)#network 10.10.10.4 0.0.0.3 area 0
core-layer3(config-router)#network 10.10.10.16 0.0.0.3 area 0
core-layer3(config-router)#network 10.10.10.28 0.0.0.3 area 0
core-layer3(config-router)#network 10.10.10.32 0.0.0.3 area 0
core-layer3(config-router)#exi
core-layer3(config-router)#exit
```

Fig.3 Routers Configuration

6- Devices Configuration

6.3 Servers

- Server Room Configuration: The server room VLAN hosts essential servers:
    - DHCP Server: Manages IP address allocation for network devices.
    - FTP Server: Hosted in the server room with limited access based on ACLs.
    - Web Server: Hosts internal and external web services.
- Servers are connected to a dedicated switch that links to the network via the FLOOR 4-ROUTER.



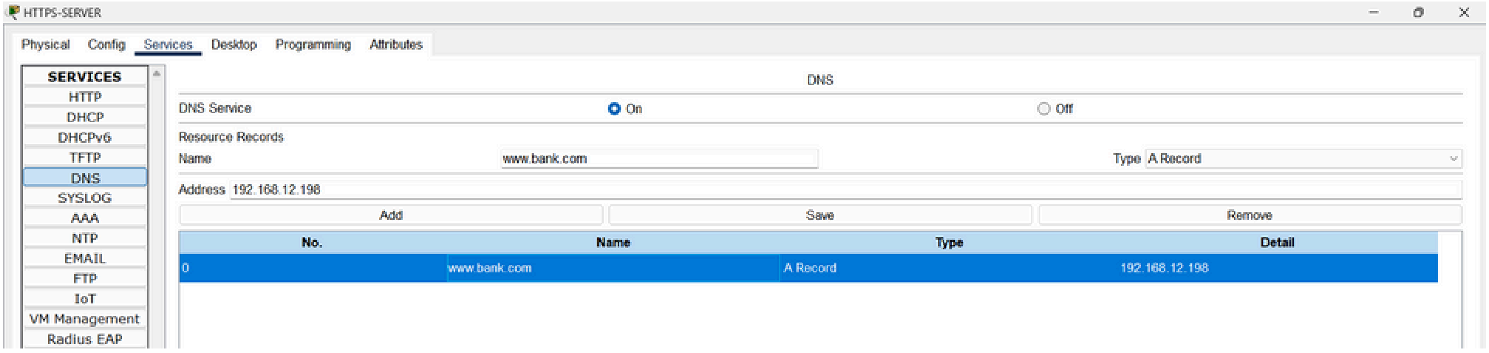
DHCP

Interface	FastEthernet0		Service ● On	○ Off
Pool Name			serverPool	
Default Gateway			0.0.0.0	
DNS Server			0.0.0.0	
Start IP Address :	192	168	12	192
Subnet Mask:	255	255	255	192
Maximum Number of Users :			64	
TFTP Server:			0.0.0.0	
WLC Address:			0.0.0.0	

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Accounts_Pool	192.168.11.1	192.168.12.198	192.168.11.5	255.255.255.192	58	0.0.0.0	0.0.0.0
LOG_Pool	192.168.11.129	192.168.12.198	192.168.11.134	255.255.255.192	58	0.0.0.0	0.0.0.0
Fin-Pool	192.168.11.65	192.168.12.198	192.168.11.70	255.255.255.192	58	0.0.0.0	0.0.0.0
CUS_Pool	192.168.11.193	192.168.12.198	192.168.11.197	255.255.255.192	58	0.0.0.0	0.0.0.0
GUSET_Pool	192.168.12.1	192.168.12.198	192.168.12.5	255.255.255.192	58	0.0.0.0	0.0.0.0
ADMIN_Pool	192.168.12.65	192.168.12.198	192.168.12.70	255.255.255.192	58	0.0.0.0	0.0.0.0
Markting_Pool	192.168.10.193	192.168.12.198	192.168.10.197	255.255.255.192	58	0.0.0.0	0.0.0.0
HR_Pool	192.168.10.129	192.168.12.198	192.168.10.134	255.255.255.192	58	0.0.0.0	0.0.0.0
Res_Pool	192.168.10.65	192.168.12.198	192.168.10.70	255.255.255.192	58	0.0.0.0	0.0.0.0
Mang_Pool	192.168.10.1	192.168.12.198	192.168.10.6	255.255.255.192	58	0.0.0.0	0.0.0.0
ICT_Pool	192.168.12.129	192.168.12.198	192.168.12.134	255.255.255.192	58	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.12.192	255.255.255.192	64	0.0.0.0	0.0.0.0

Fig.4 DHCP Server Configuration

6- Devices Configuration



DNS

DNS Service ● On ○ Off

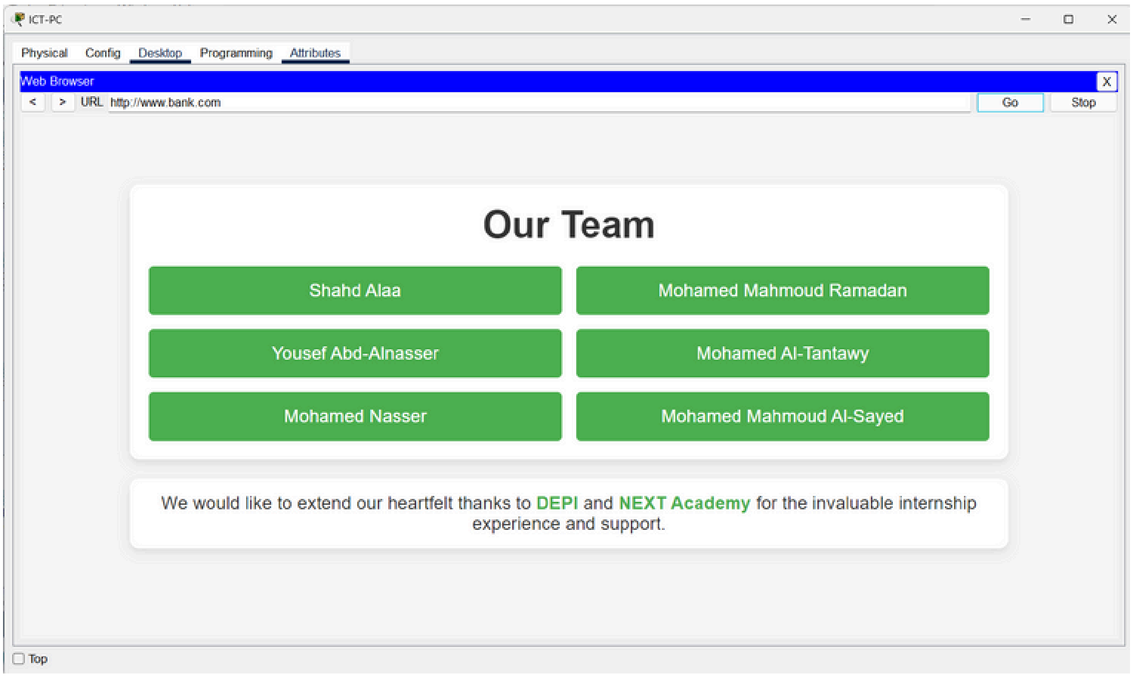
Resource Records

Name www.bank.com Type A Record

Address 192.168.12.198

No.	Name	Type	Detail
0	www.bank.com	A Record	192.168.12.198

Fig.2 DNS Server



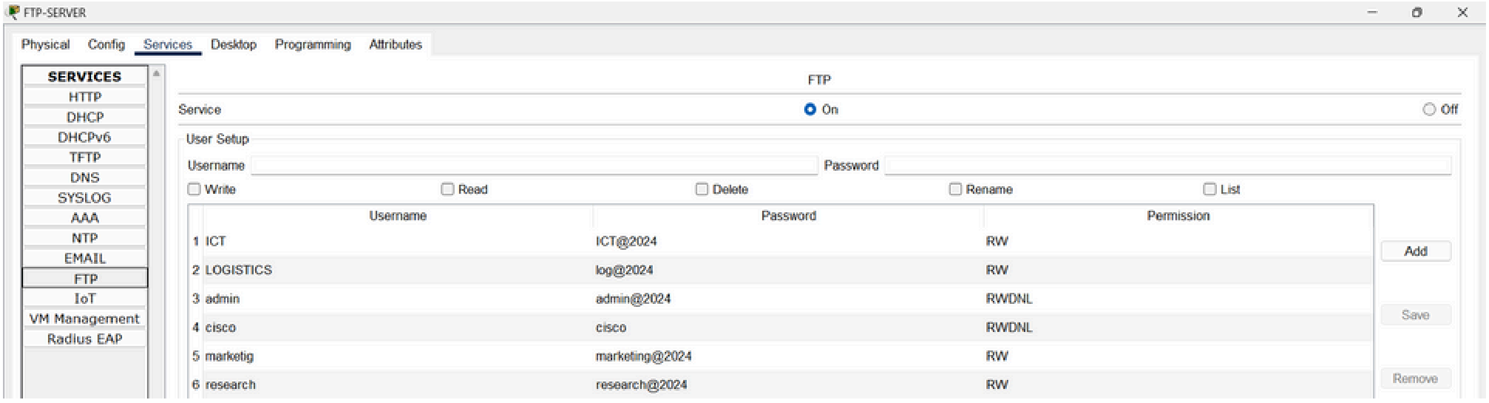
URL http://www.bank.com

Our Team

Shahd Alaa	Mohamed Mahmoud Ramadan
Yousef Abd-Alnasser	Mohamed Al-Tantawy
Mohamed Nasser	Mohamed Mahmoud Al-Sayed

We would like to extend our heartfelt thanks to DEPI and NEXT Academy for the invaluable internship experience and support.

Fig.5 HTTP Server



FTP

Service ● On ○ Off

User Setup

Username Password

□ Write □ Read □ Delete □ Rename □ List

	Username	Password	Permission
1	ICT	ICT@2024	RW
2	LOGISTICS	log@2024	RW
3	admin	admin@2024	RWDNL
4	cisco	cisco	RWDNL
5	marketig	marketing@2024	RW
6	research	research@2024	RW

Fig.6 FTP Server Configuration

7- IP Addressing Scheme

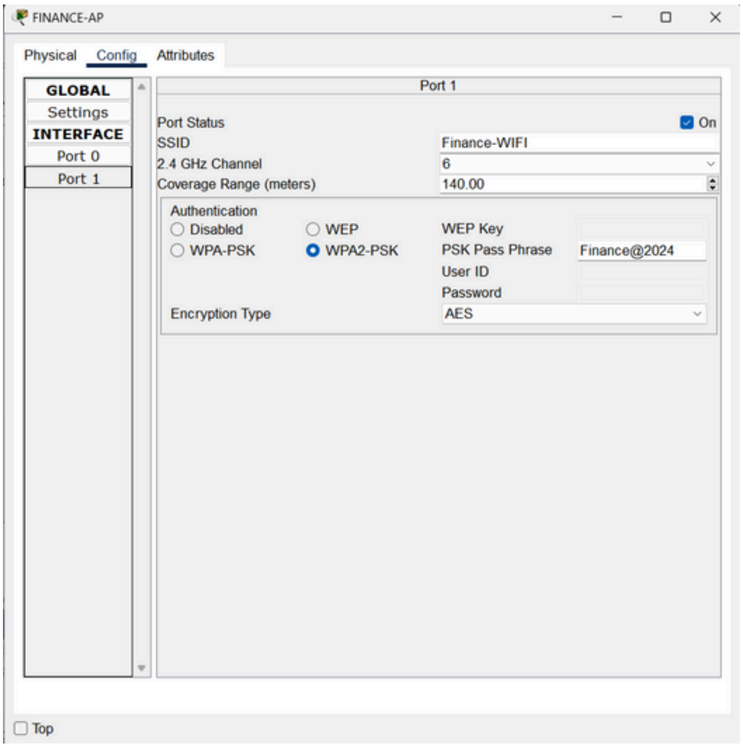
The IP addressing follows a hierarchical scheme to facilitate easy management and troubleshooting:

1. Management VLAN (10): 192.168.10.0/26
    - Default Gateway: 192.168.10.1
2. Research VLAN (20): 192.168.10.64/26
    - Default Gateway: 192.168.10.65
3. Human Resources VLAN (30): 192.168.10.128/26
    - Default Gateway: 192.168.10.129
4. Marketing VLAN (40): 192.168.10.192/26
    - Default Gateway: 192.168.10.193
5. Accounts VLAN (50): 192.168.11.0/26
    - Default Gateway: 192.168.11.1
6. Finance VLAN (60): 192.168.11.64/26
    - Default Gateway: 192.168.11.65
7. Logistics VLAN (70): 192.168.11.128/26
    - Default Gateway: 192.168.11.129
8. Customer Service VLAN (80): 192.168.11.192/26
    - Default Gateway: 192.168.11.193
9. Guests VLAN (90): 192.168.12.0/26
    - Default Gateway: 192.168.12.1
10. Administration VLAN (100): 192.168.12.64/26
    - Default Gateway: 192.168.12.65
11. Information Technology VLAN (110): 192.168.12.128/26
    - Default Gateway: 192.168.12.129
12. Server Room VLAN (120): 192.168.12.192/26
    - Default Gateway: 192.168.12.193

8- Wireless Network Design

Each floor is equipped with wireless access points configured for different VLANs:

- SSID Configuration:
  - Management-WiFi (VLAN 10)
  - Guest-WiFi (VLAN 90)
  - Department-specific SSIDs corresponding to each VLAN.
- Security: WPA2 encryption is used across all SSIDs to ensure secure wireless connections.



Port 1

Port Status ☑ On

SSID Finance-WIFI

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key

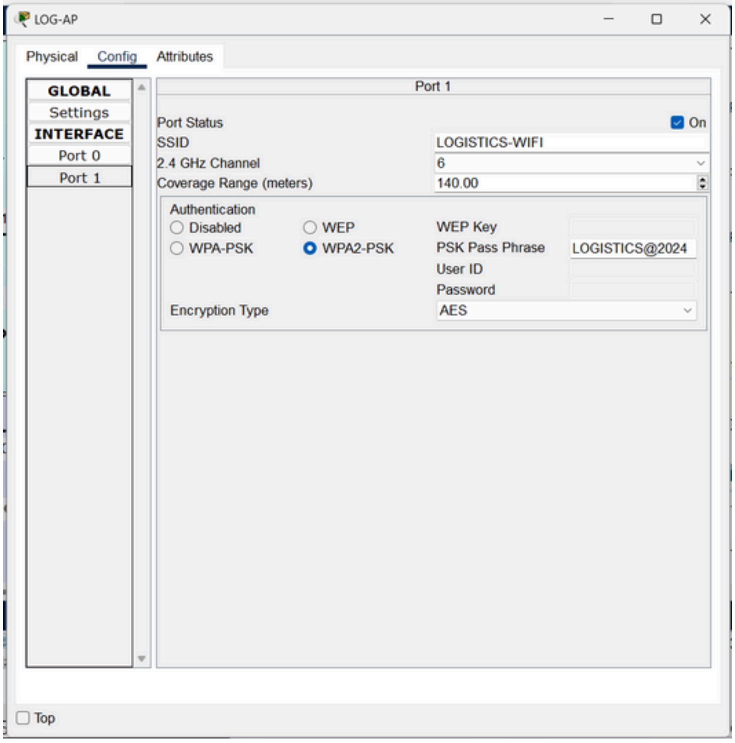
PSK Pass Phrase Finance@2024

User ID

Password

Encryption Type AES

Fig.7 Finance Dept AP Config



Port 1

Port Status ☑ On

SSID LOGISTICS-WIFI

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key

PSK Pass Phrase LOGISTICS@2024

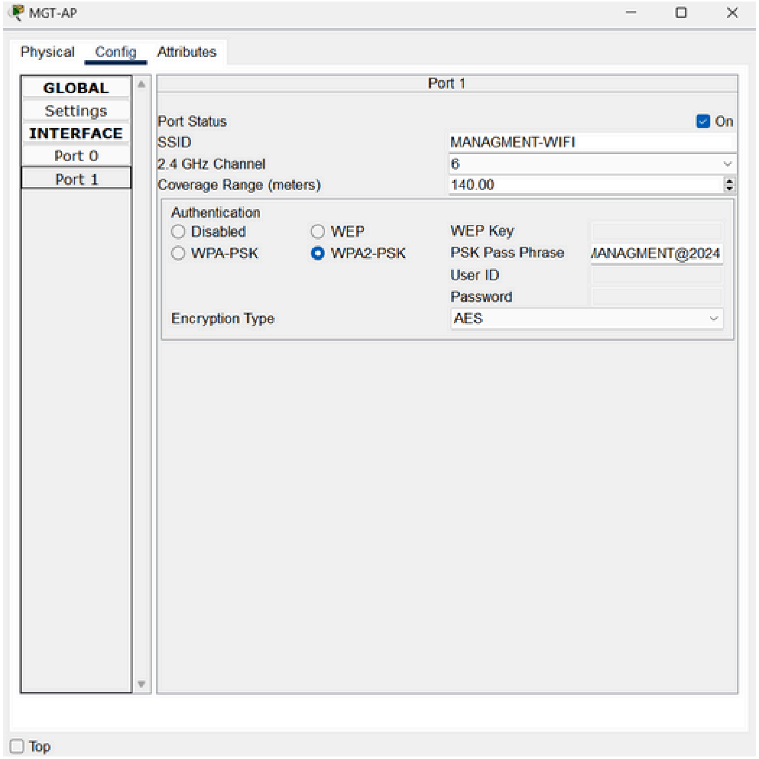
User ID

Password

Encryption Type AES

Fig.8 Logistics Dept AP Config

8- Wireless Network Design



Port 1

Port Status ☑ On

SSID: MANAGMENT-WIFI

2.4 GHz Channel: 6

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

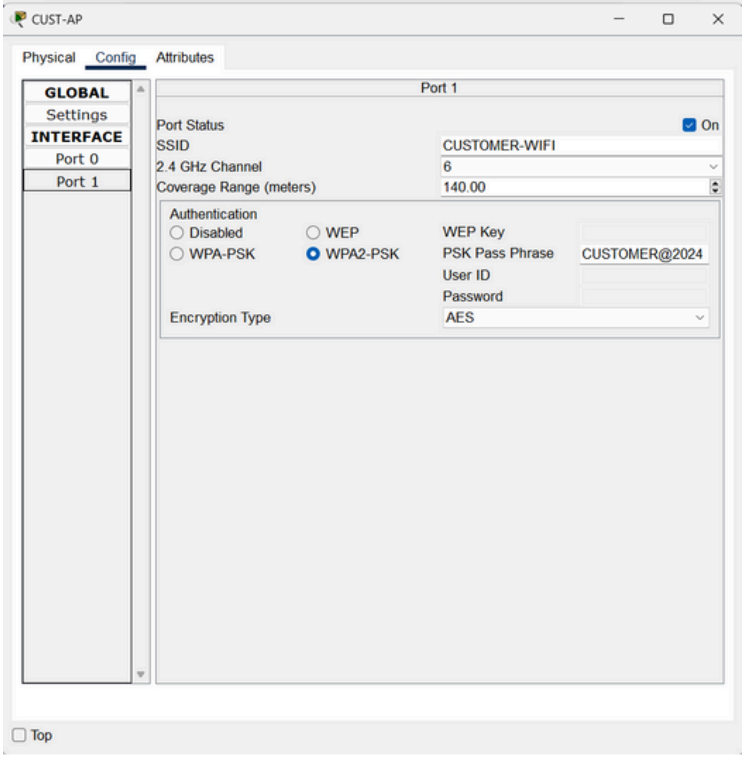
WEP Key:

PSK Pass Phrase: IANAGMENT@2024

User ID:

Password:

Encryption Type: AES



Port 1

Port Status ☑ On

SSID: CUSTOMER-WIFI

2.4 GHz Channel: 6

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: CUSTOMER@2024

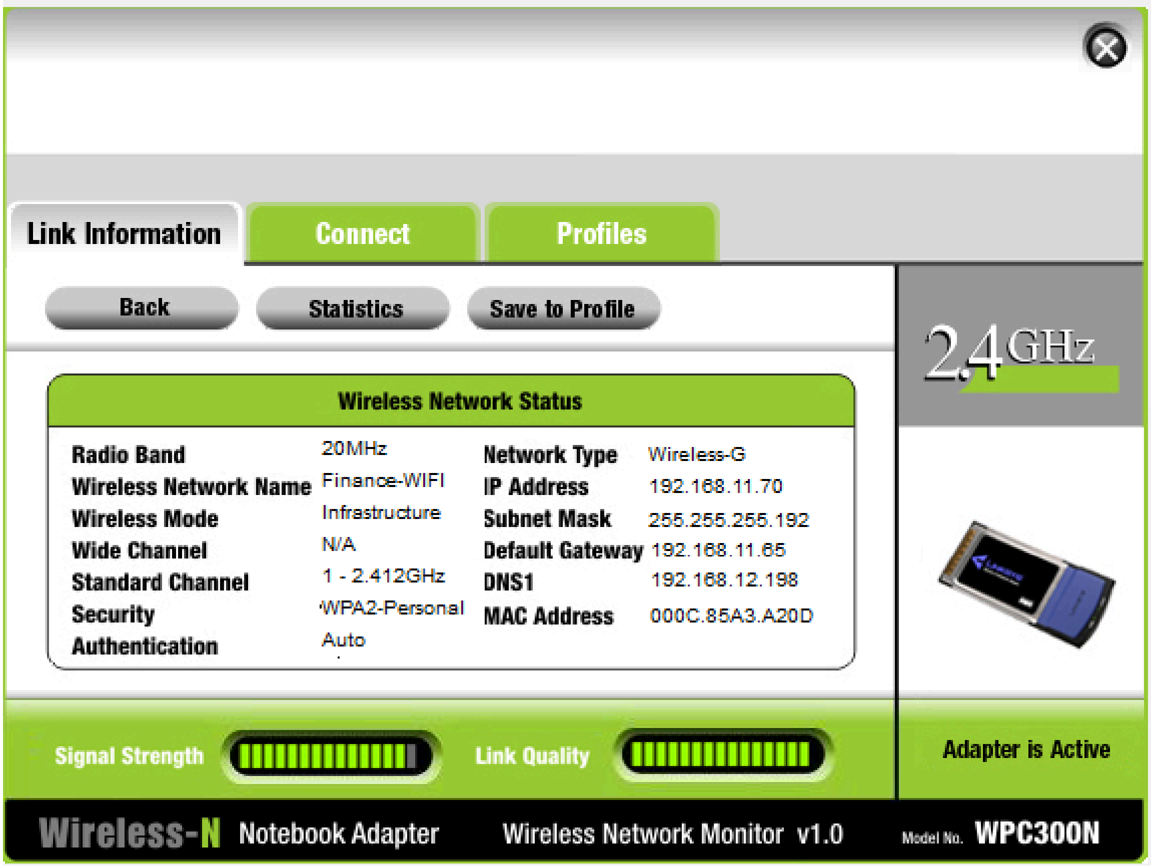
User ID:

Password:

Encryption Type: AES

Fig.9 Management Dept AP

Fig.10 Customers Dept AP



Wireless Network Status

Radio Band	20MHz	Network Type	Wireless-G
Wireless Network Name	Finance-WIFI	IP Address	192.168.11.70
Wireless Mode	Infrastructure	Subnet Mask	255.255.255.192
Wide Channel	N/A	Default Gateway	192.168.11.65
Standard Channel	1 - 2.412GHz	DNS1	192.168.12.198
Security	WPA2-Personal	MAC Address	000C.85A3.A20D
Authentication	Auto		

Adapter is Active

Fig.11 Laptop Connection Status

9- Redundancy and Failover

The network is designed with multiple layers of redundancy:

- Router Redundancy: Multiple routers provide alternate paths for traffic.
- Link Redundancy: Dual links between routers and switches ensure continued operation if a single link fails.
- Spanning Tree Protocol (STP): Configured to prevent loops while maintaining redundancy.

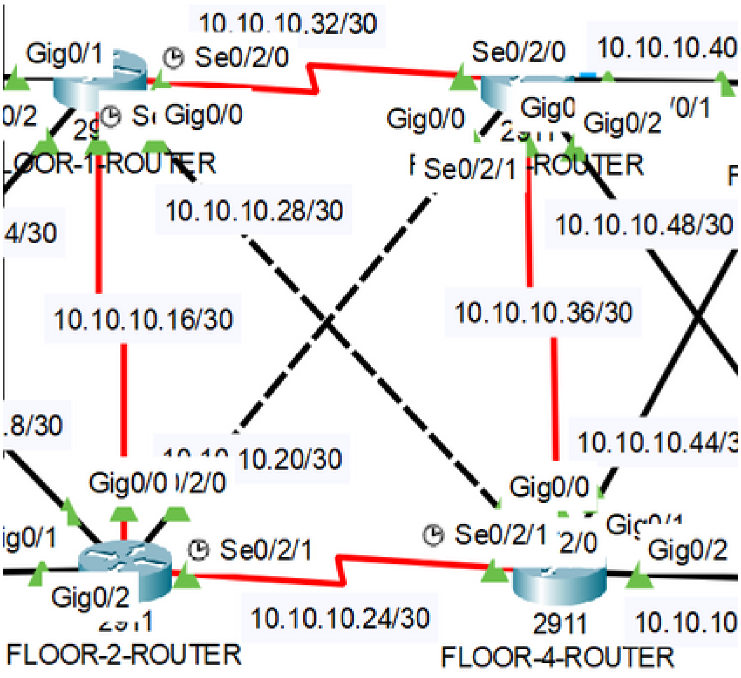


Fig.12 Routers Redundancy

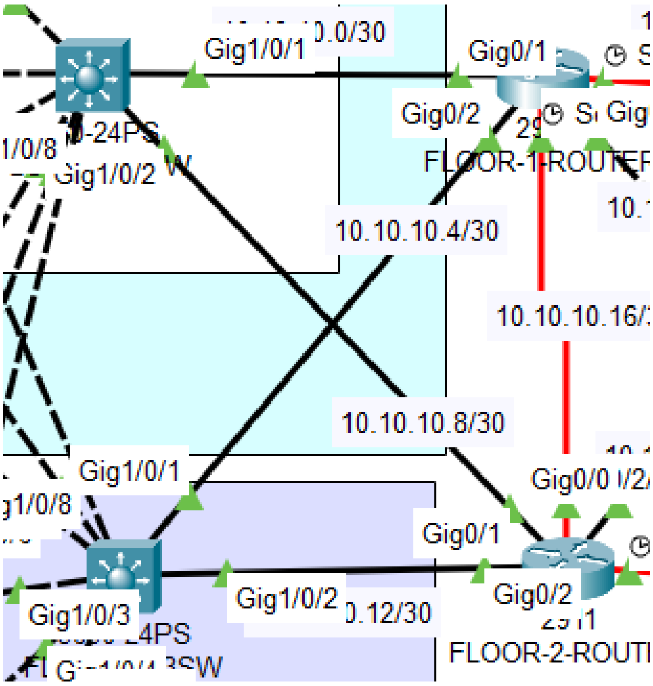


Fig.13 Multi-Layer SW Redundancy

10- Project Final Testing

The final testing phase ensures that the network design and implementation meet the project’s requirements and function as intended. The testing process involves validating the overall design and ensuring full connectivity across the network.

1- Overall Design Testing:

- Objective: To verify that the network architecture aligns with the original design specifications, including VLAN segmentation, routing configurations, redundancy protocols, and security policies.
- Key Testing Steps:
  - VLAN Segmentation Validation: Ensure that all VLANs are properly configured, with correct IP addressing and VLAN IDs.
  - Inter-VLAN Routing Verification: Test communication between different VLANs to confirm that inter-VLAN routing on multilayer switches is functioning as intended.
  - Redundancy and Failover Testing: Simulate link or device failures to ensure that redundancy protocols (e.g., HSRP) maintain network availability.
  - Security Policy Enforcement: Confirm that ACLs and port security measures are correctly implemented to restrict unauthorized access.

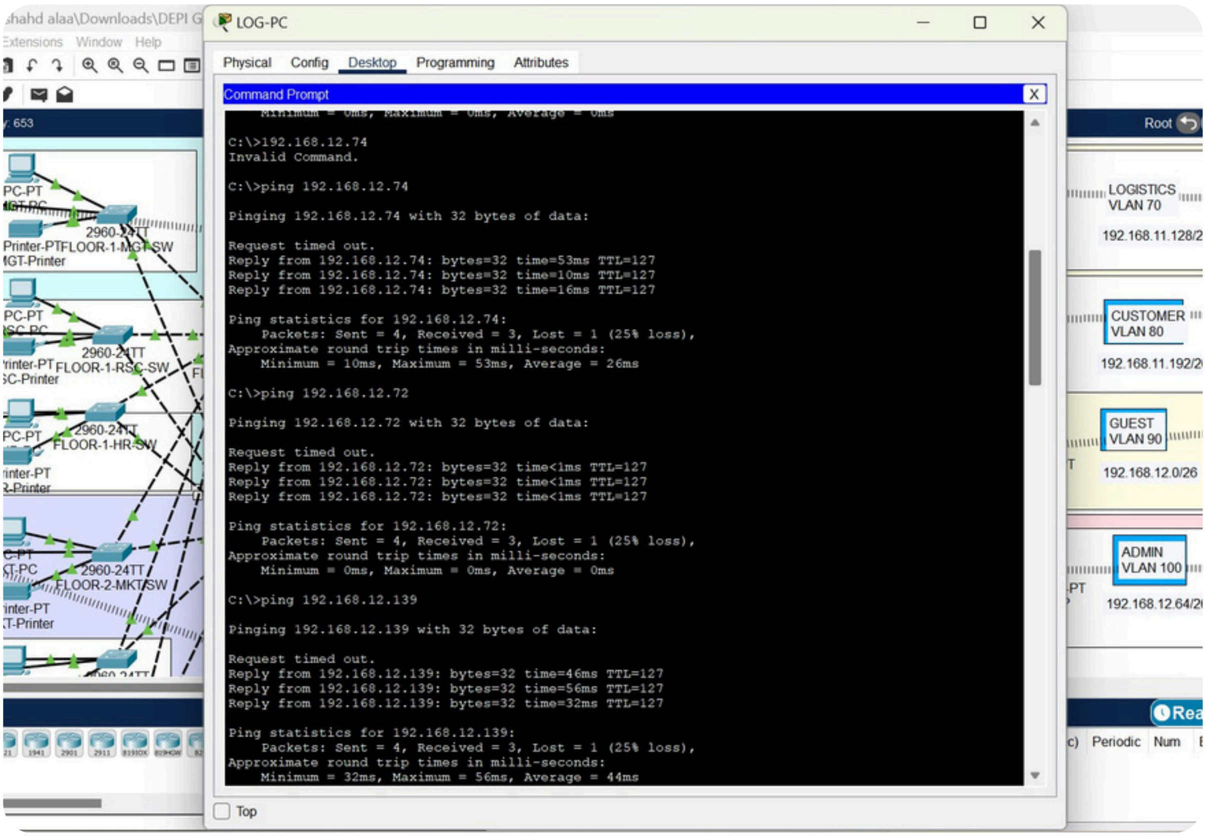
10- Project Final Testing

2- Connectivity Testing

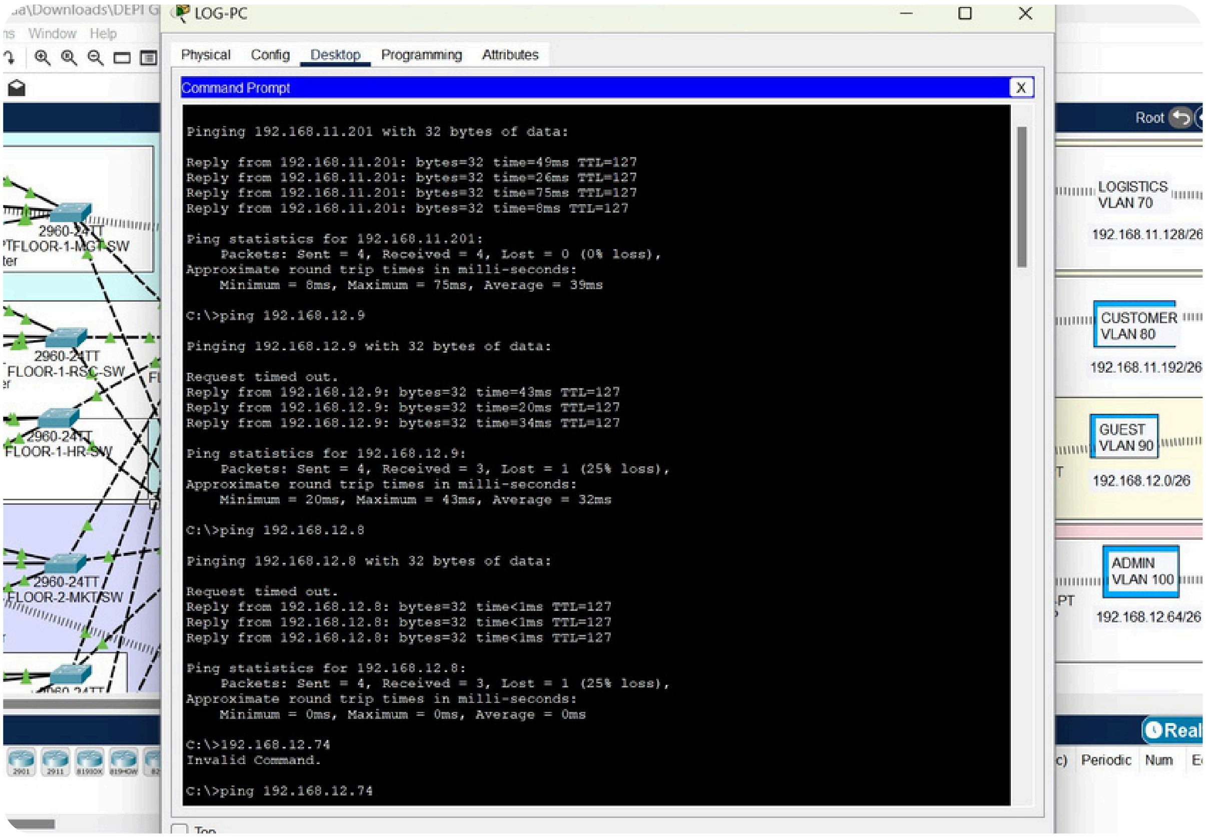
- Objective: To test end-to-end connectivity across the network, ensuring that all devices can communicate as per the network design.
- Key Testing Steps:
    - Ping Tests: Conduct ping tests to check connectivity between devices on the same VLAN, as well as across different VLANs, to confirm proper routing.
    - Service Access Testing: Verify access to network services (e.g., FTP server, DHCP, email) from various VLANs based on access control policies.
    - Device Connectivity Verification: Test the connectivity of end-user devices (PCs, printers, IP phones) and wireless access points to ensure they can connect to the network.
    - Network Performance Monitoring: Measure network latency, throughput, and packet loss during peak and normal operation conditions to ensure the network performs within acceptable limits.

The project final testing phase is crucial for identifying any configuration issues or potential improvements before the network is fully deployed. This ensures a stable and efficient network environment for the bank.

10- Project Final Testing



```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>192.168.12.74
Invalid Command.

C:\>ping 192.168.12.74

Pinging 192.168.12.74 with 32 bytes of data:

Request timed out.
Reply from 192.168.12.74: bytes=32 time=53ms TTL=127
Reply from 192.168.12.74: bytes=32 time=10ms TTL=127
Reply from 192.168.12.74: bytes=32 time=16ms TTL=127

Ping statistics for 192.168.12.74:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 53ms, Average = 26ms

C:\>ping 192.168.12.72

Pinging 192.168.12.72 with 32 bytes of data:

Request timed out.
Reply from 192.168.12.72: bytes=32 time<1ms TTL=127
Reply from 192.168.12.72: bytes=32 time<1ms TTL=127
Reply from 192.168.12.72: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.12.72:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.12.139

Pinging 192.168.12.139 with 32 bytes of data:

Request timed out.
Reply from 192.168.12.139: bytes=32 time=46ms TTL=127
Reply from 192.168.12.139: bytes=32 time=56ms TTL=127
Reply from 192.168.12.139: bytes=32 time=32ms TTL=127

Ping statistics for 192.168.12.139:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 56ms, Average = 44ms
```

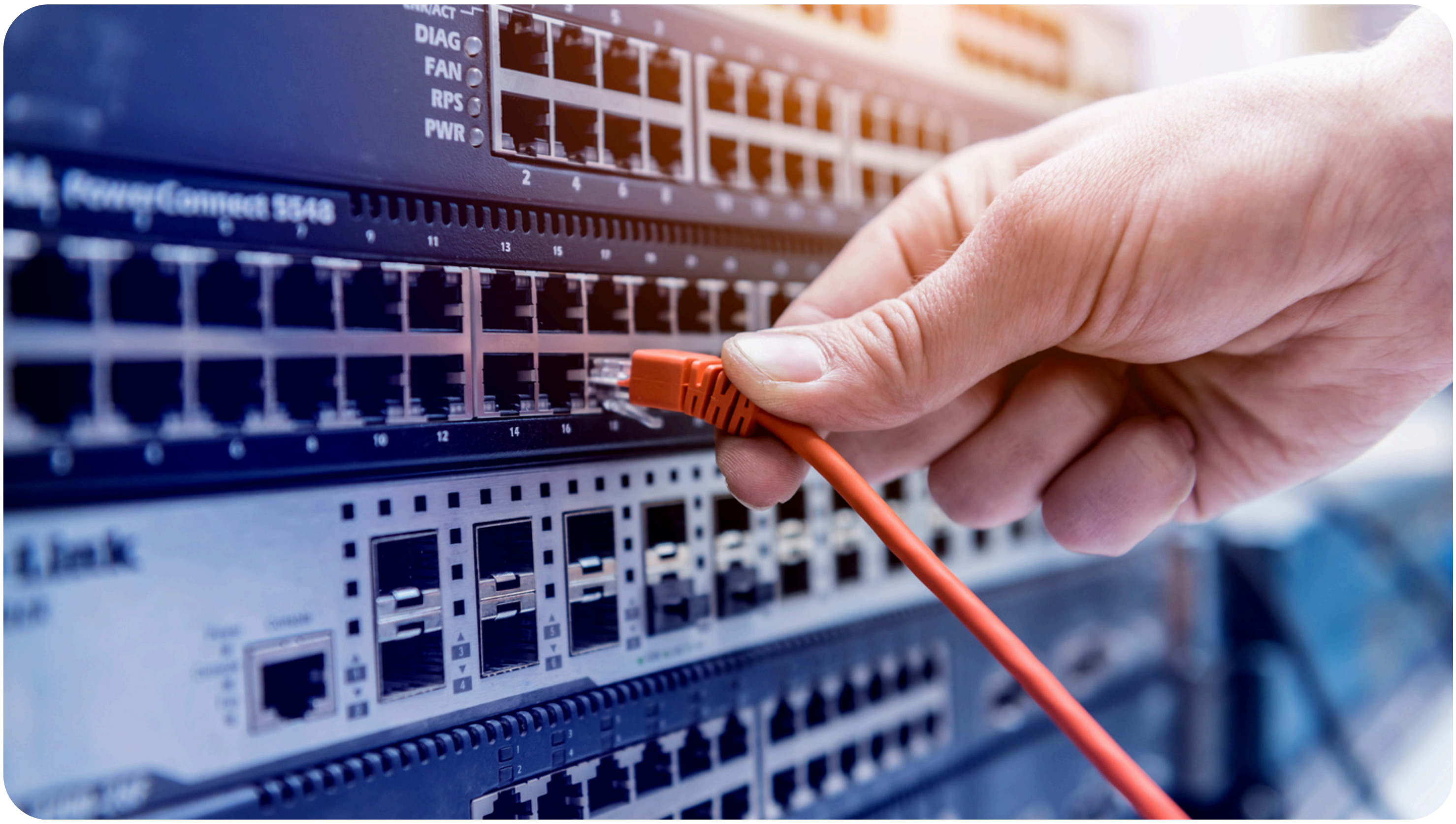


```
Pinging 192.168.11.201 with 32 bytes of data:

Reply from 192.168.11.201: bytes=32 time=49ms TTL=127
Reply from 192.168.11.201: bytes=32 time=26ms TTL=127
Reply from 192.168.11.201: bytes=32 time=75ms TTL=127
Reply from 192.168.11.201: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.11.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 75ms, Average = 39ms

C:\>ping 192.168.12.9

Pinging 192.168.12.9 with 32 bytes of data:

Request timed out.
Reply from 192.168.12.9: bytes=32 time=43ms TTL=127
Reply from 192.168.12.9: bytes=32 time=20ms TTL=127
Reply from 192.168.12.9: bytes=32 time=34ms TTL=127

Ping statistics for 192.168.12.9:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 43ms, Average = 32ms

C:\>ping 192.168.12.8

Pinging 192.168.12.8 with 32 bytes of data:

Request timed out.
Reply from 192.168.12.8: bytes=32 time<1ms TTL=127
Reply from 192.168.12.8: bytes=32 time<1ms TTL=127
Reply from 192.168.12.8: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.12.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>192.168.12.74
Invalid Command.

C:\>ping 192.168.12.74
```

Fig.14 Connectivity Testing

11- Conclusion

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



Thank You!