# Cisco Packet Tracer Project - Enterprise Network Security and Configuration

*By Lucio Rodrigues*

## Introduction

This project focuses on designing and configuring a **multi-floor enterprise network** in Cisco Packet Tracer. It simulates the process of building a secure, scalable, and functional infrastructure that supports multiple departments, centralised services, wireless connectivity, and internet access.

From a technical perspective, the project integrates key networking concepts such as VLANs, OSPF routing, DHCP services, NAT/PAT, ACLs, wireless configuration, and port security. Each of these elements mirrors the tasks a network engineer or cybersecurity analyst would encounter when managing or defending real-world environments.

From a **cybersecurity perspective**, this project is highly valuable because it teaches:

- **Network Segmentation & VLANs** → Understanding how isolating departments limits the impact of attacks.
- **Switchport Security & ACLs** → Applying access restrictions at the network edge to reduce the attacker's window of opportunity.
- **Routing & DHCP** → Identifying common misconfigurations that attackers exploit for lateral movement or privilege escalation.
- **NAT/PAT & Default Routes** → Observing how traffic flows to and from the internet, which directly relates to monitoring, intrusion detection, and firewall placement.
- **End-to-End Verification** → Practicing how to validate configurations with pings, SSH sessions, and service checks, just like a blue teamer would during incident response.

By completing this project, you not only gain the technical skills to configure enterprise-grade networks but also strengthen your **defensive mindset**, understanding where vulnerabilities may arise, and how security measures align with core network functions.

## ✅ Completed Project Overview

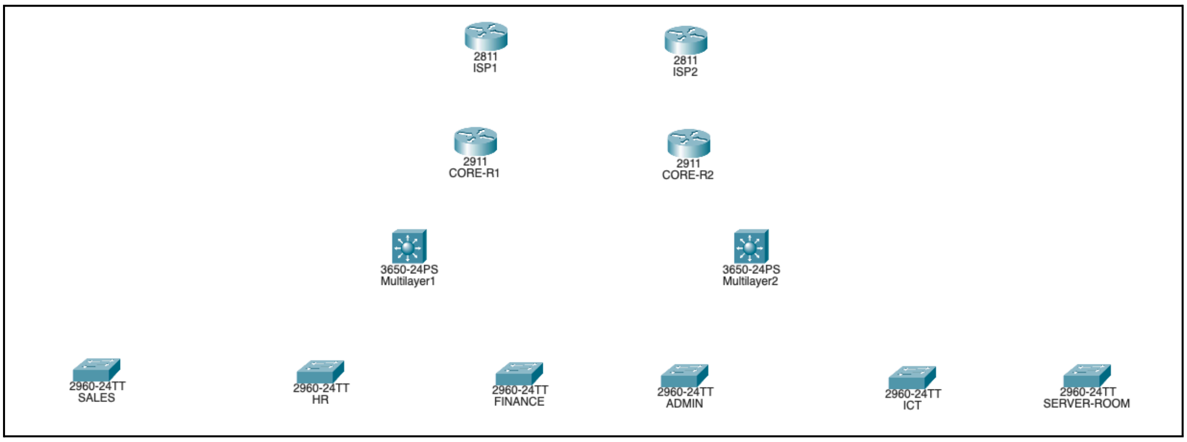
Upon completion of this project, the enterprise network is fully operational across three floors, with secure segmentation and centralised services in place. Each department operates within its own VLAN, supported by OSPF dynamic routing and inter-VLAN connectivity through Layer 3 switching. DHCP provides automated IP assignments, while static IPs are reserved for servers and critical devices.

Network security is reinforced with switchport security in the Finance department, ACLs controlling traffic flow, and PAT providing secure internet access for internal hosts. Wireless users are seamlessly integrated into the network with WPA2-protected access. A default static route ensures connectivity to the ISP, enabling controlled external communication.

Verification tests confirm reliable end-to-end connectivity, proper VLAN segmentation, dynamic address distribution, secure remote access via SSH, and successful traffic translation to the public internet. The result is a scalable, secure, and enterprise-ready network that closely mirrors real-world environments and reinforces both networking and cybersecurity skills.

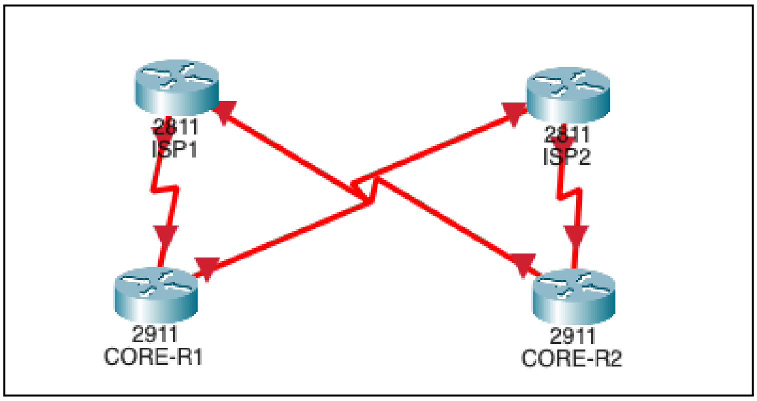
**Figures:**

*Initial Setup.*



***Cisco 2911** routers were used as the enterprise edge routers, while **Cisco 2811** routers were used to simulate the ISP routers. This separation reflects real-world scenarios where different router classes are deployed for internal vs. provider roles.*

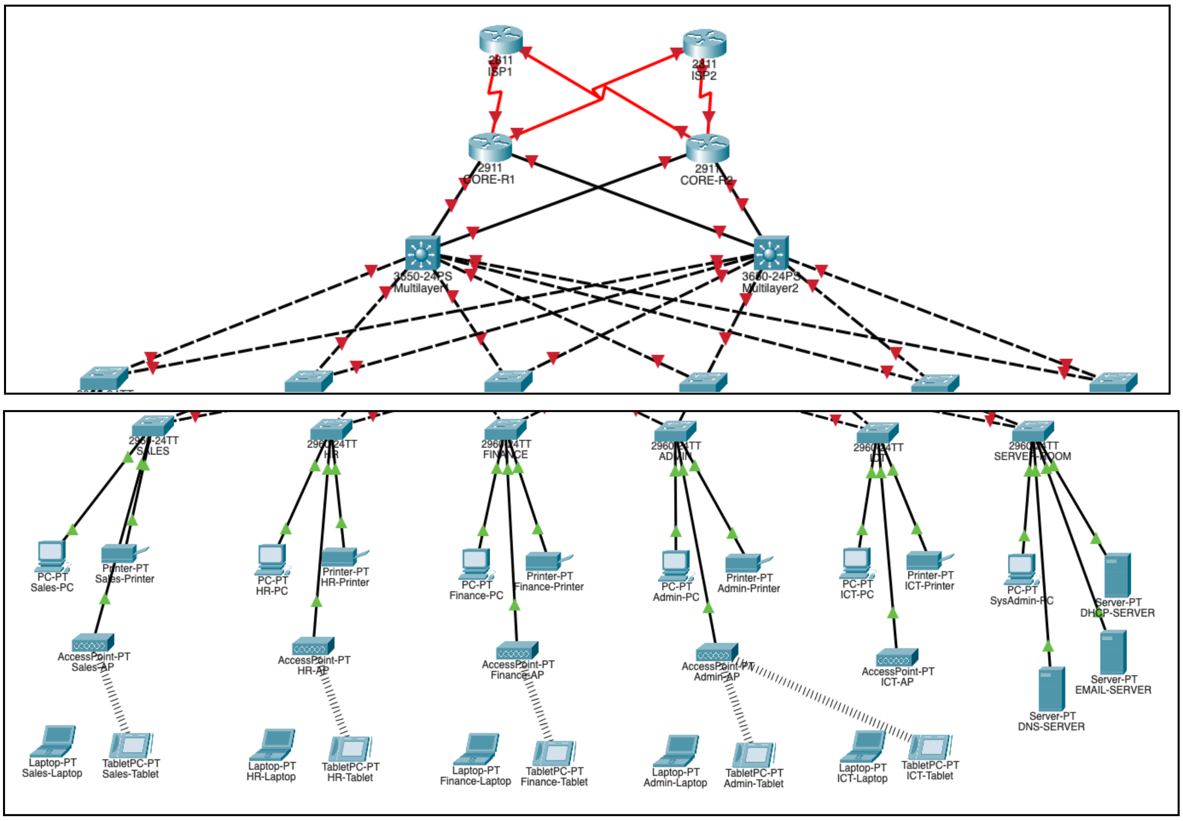
***Multilayer switches** were used at the distribution layer to handle both switching and inter-VLAN routing. This design improves performance and enables OSPF participation for redundancy. Regular Layer 2 switches were used at the access layer to connect end devices and wireless APs.*



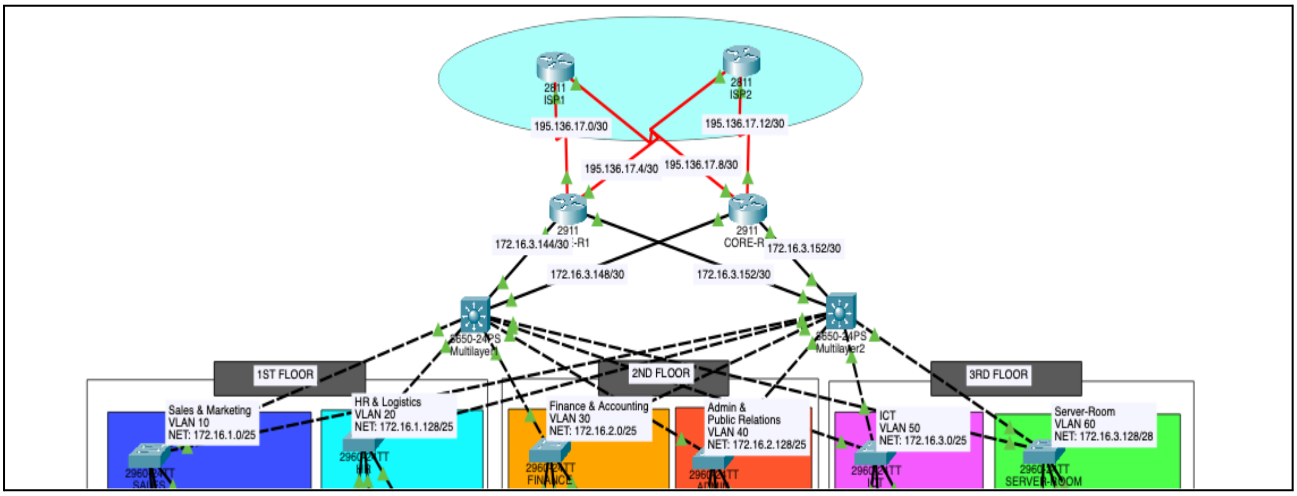
*Two separate ISPs were connected to the enterprise routers to eliminate single points of failure and guarantee continuous internet access. This design ensures business continuity for critical departments such as Finance and Sales, where downtime could result in financial losses.*

*Additionally, dual ISP connections allow for load sharing, improved performance, and alignment with industry best practices for redundancy in financial institutions.*

*Setup before configurations.*



*The complete enterprise network with ISP connectivity, routers, multilayer switches, and departmental subnets across three floors.*



## ⚙️ Configuration Steps

The network was built and secured using the following configuration steps:

1. Apply basic settings to all devices, including SSH on routers and Switch 13.
2. Configure VLANs, and assign access and trunk ports on Switches 12 and 13.
3. Implement switchport security for the Finance department.
4. Perform subnetting and assign IP addresses.
5. Configure OSPF on the routers and Switch 13.
6. Assign static IP addresses to Server Room devices.
7. Configure the DHCP server and related settings.
8. Set up inter-VLAN routing on Switch 13 and apply IP DHCP helper addresses.
9. Configure the wireless network.
10. Implement Port Address Translation (PAT) and Access Control Lists (ACLs).
11. Apply a default static route.
12. Verify and test all configurations.

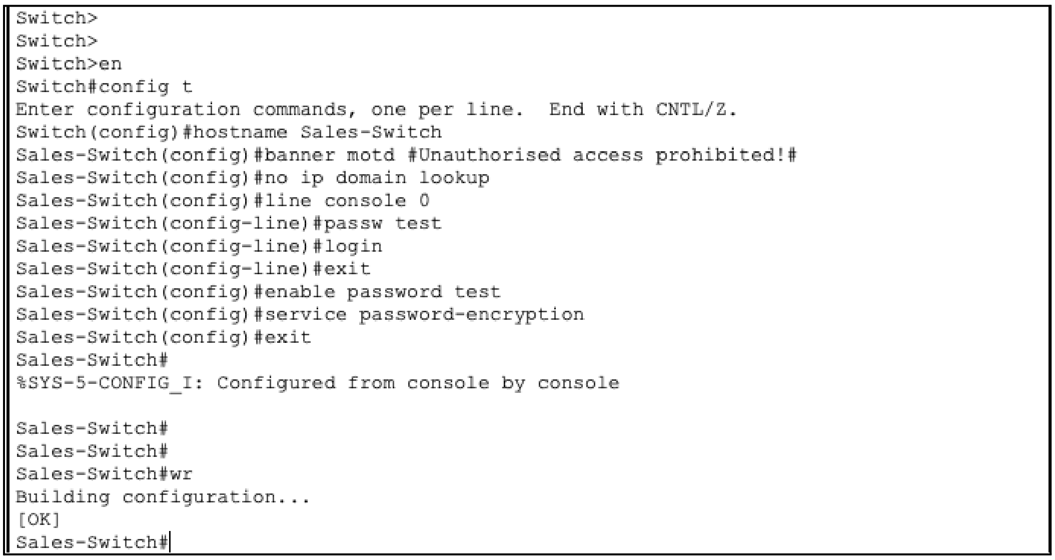
This tutorial provides the full configuration process for the Packet Tracer project, including VLANs, routing, DHCP, wireless setup, security, and final testing.

# 1. Basic Settings (All Devices + SSH)

- Set hostname
- Set console and VTY passwords
- Configure enable secret
- Configure SSH (Routers + Switch 13)

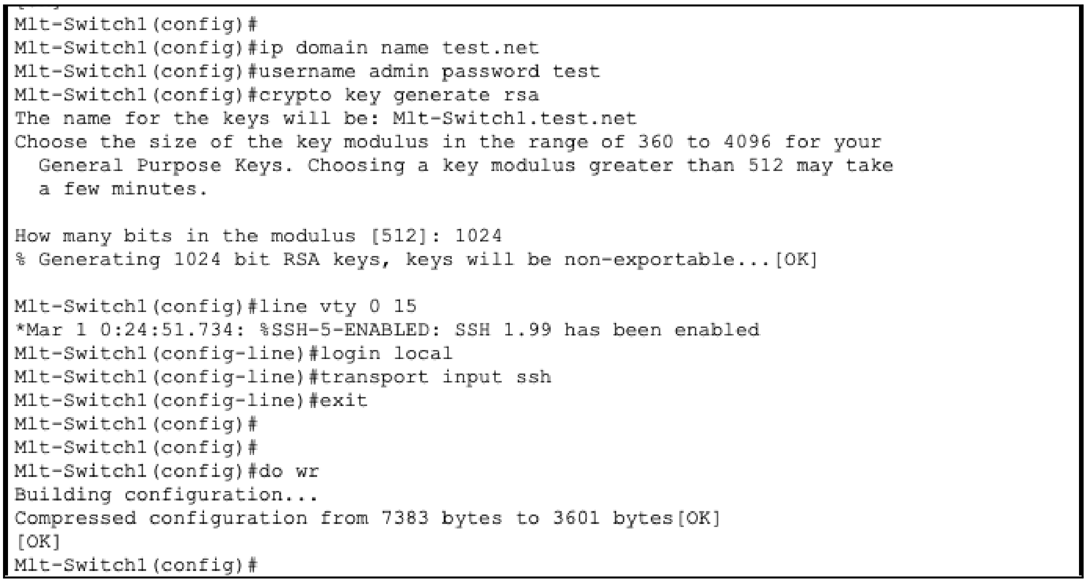
**Figures:**

*Hostname, banner, password configured.*



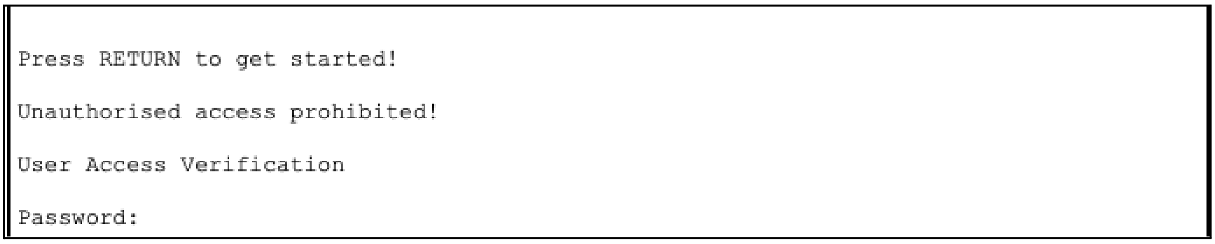
```
Switch>
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sales-Switch
Sales-Switch(config)#banner motd #Unauthorised access prohibited!#
Sales-Switch(config)#no ip domain lookup
Sales-Switch(config)#line console 0
Sales-Switch(config-line)#passw test
Sales-Switch(config-line)#login
Sales-Switch(config-line)#exit
Sales-Switch(config)#enable password test
Sales-Switch(config)#service password-encryption
Sales-Switch(config)#exit
Sales-Switch#
%SYS-5-CONFIG_I: Configured from console by console

Sales-Switch#
Sales-Switch#
Sales-Switch#wr
Building configuration...
[OK]
Sales-Switch#
```

*SSH configuration on multilayer switch.*



```
Mlt-Switch1(config)#
Mlt-Switch1(config)#ip domain name test.net
Mlt-Switch1(config)#username admin password test
Mlt-Switch1(config)#crypto key generate rsa
The name for the keys will be: Mlt-Switch1.test.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]

Mlt-Switch1(config)#line vty 0 15
*Mar 1 0:24:51.734: %SSH-5-ENABLED: SSH 1.99 has been enabled
Mlt-Switch1(config-line)#login local
Mlt-Switch1(config-line)#transport input ssh
Mlt-Switch1(config-line)#exit
Mlt-Switch1(config)#
Mlt-Switch1(config)#
Mlt-Switch1(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Mlt-Switch1(config)#
```

*SSH configured.*

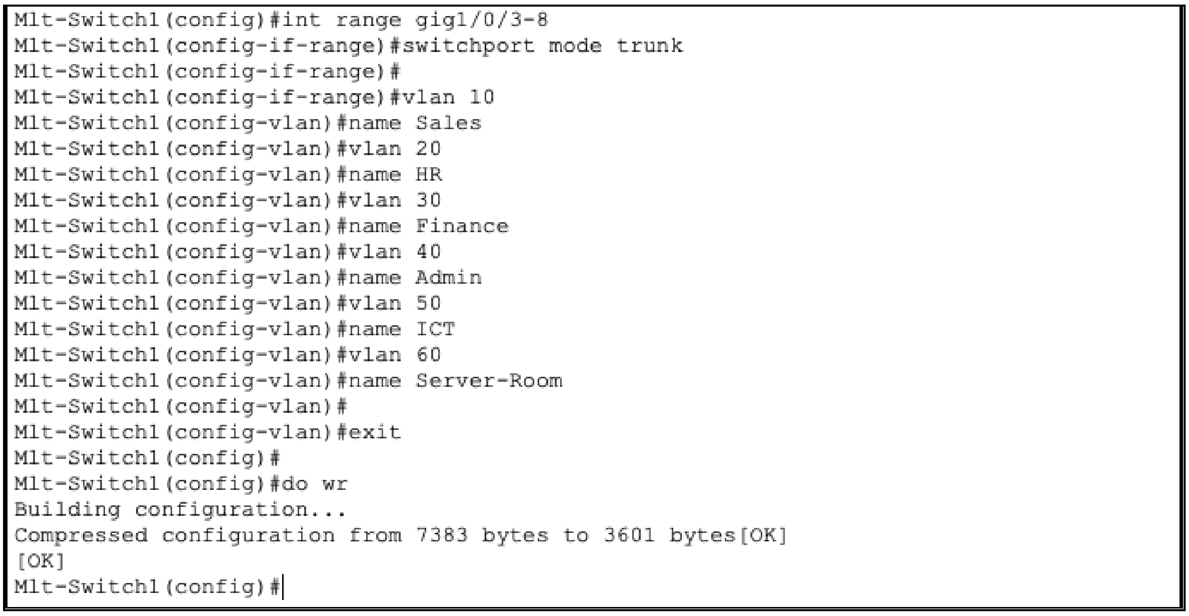


```
Press RETURN to get started!

Unauthorised access prohibited!

User Access Verification

Password:
```

## 2. VLAN Creation and Port Assignment (Switches 12 & 13)

- Create VLANs (e.g., VLAN 10 = Sales, VLAN 20 = Finance, VLAN 30 = Management)
- Assign access ports to VLANs
- Configure trunk ports between switches

*VLANs creation & trunk ports.*



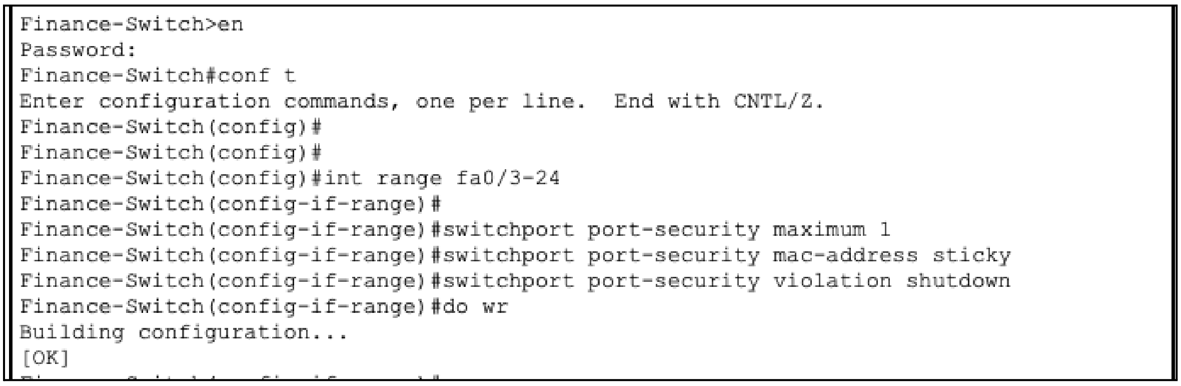
```
Mlt-Switch1(config)#int range gig1/0/3-8
Mlt-Switch1(config-if-range)#switchport mode trunk
Mlt-Switch1(config-if-range)#
Mlt-Switch1(config-if-range)#vlan 10
Mlt-Switch1(config-vlan)#name Sales
Mlt-Switch1(config-vlan)#vlan 20
Mlt-Switch1(config-vlan)#name HR
Mlt-Switch1(config-vlan)#vlan 30
Mlt-Switch1(config-vlan)#name Finance
Mlt-Switch1(config-vlan)#vlan 40
Mlt-Switch1(config-vlan)#name Admin
Mlt-Switch1(config-vlan)#vlan 50
Mlt-Switch1(config-vlan)#name ICT
Mlt-Switch1(config-vlan)#vlan 60
Mlt-Switch1(config-vlan)#name Server-Room
Mlt-Switch1(config-vlan)#
Mlt-Switch1(config-vlan)#exit
Mlt-Switch1(config)#
Mlt-Switch1(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Mlt-Switch1(config)#
```

# 3. Switchport Security (Finance Department)

- Enable port security on Finance PCs
- Set maximum MAC addresses
- Enable violation mode (shutdown)

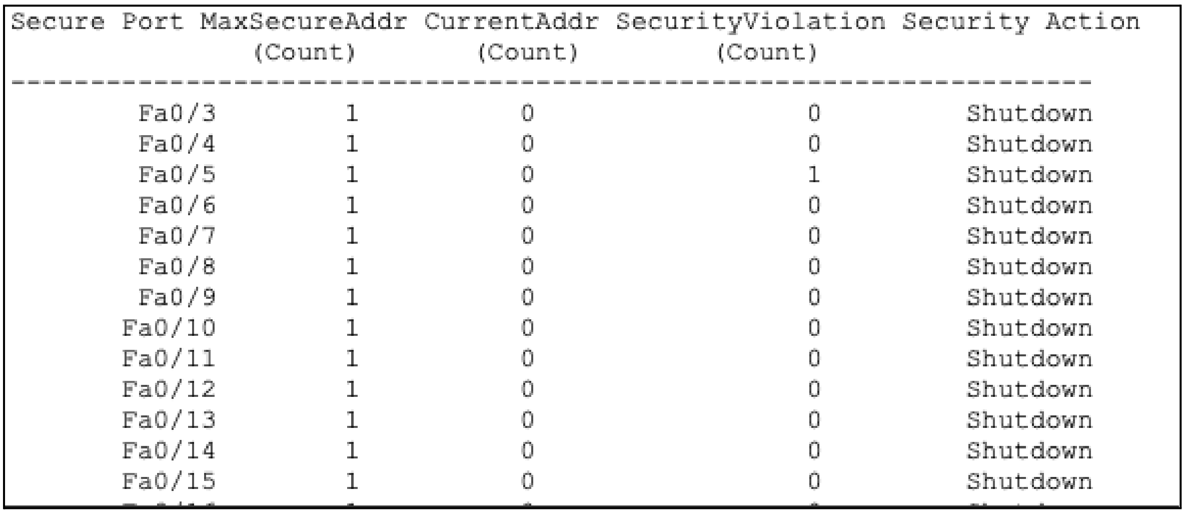
**Figures:**

*Switchport security configuration.*



```
Finance-Switch>en
Password:
Finance-Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Finance-Switch(config)#
Finance-Switch(config)#
Finance-Switch(config)#int range fa0/3-24
Finance-Switch(config-if-range)#
Finance-Switch(config-if-range)#switchport port-security maximum 1
Finance-Switch(config-if-range)#switchport port-security mac-address sticky
Finance-Switch(config-if-range)#switchport port-security violation shutdown
Finance-Switch(config-if-range)#do wr
Building configuration...
[OK]
```

*Run command “do show port-security”.*



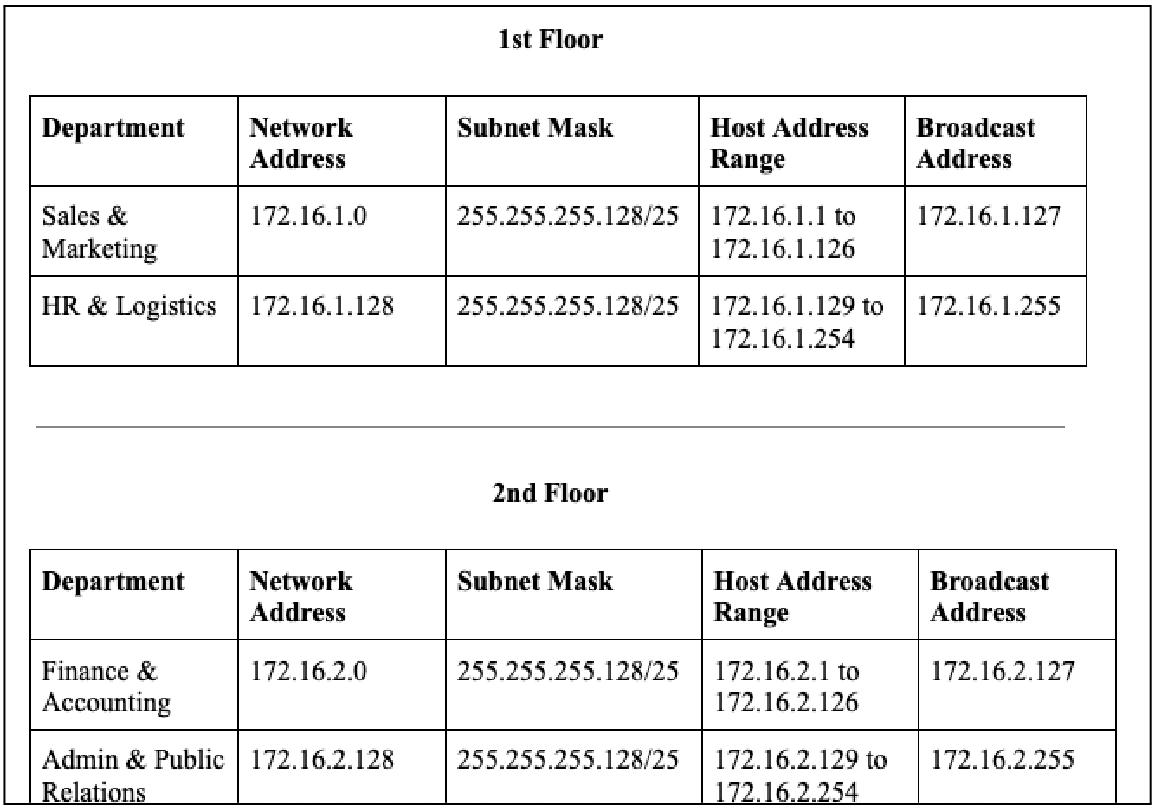
```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/3        1           0                 0         Shutdown
        Fa0/4        1           0                 0         Shutdown
        Fa0/5        1           0                 1         Shutdown
        Fa0/6        1           0                 0         Shutdown
        Fa0/7        1           0                 0         Shutdown
        Fa0/8        1           0                 0         Shutdown
        Fa0/9        1           0                 0         Shutdown
       Fa0/10        1           0                 0         Shutdown
       Fa0/11        1           0                 0         Shutdown
       Fa0/12        1           0                 0         Shutdown
       Fa0/13        1           0                 0         Shutdown
       Fa0/14        1           0                 0         Shutdown
       Fa0/15        1           0                 0         Shutdown
```

# 4. Subnetting & IP Addressing

- Document the subnet plan
- Assign IPs to router interfaces and switch SVIs
- Assign IPs to PCs, servers, and printers

**Figures:**

*The complete list of IP addresses can be found in the Network Configuration file.*



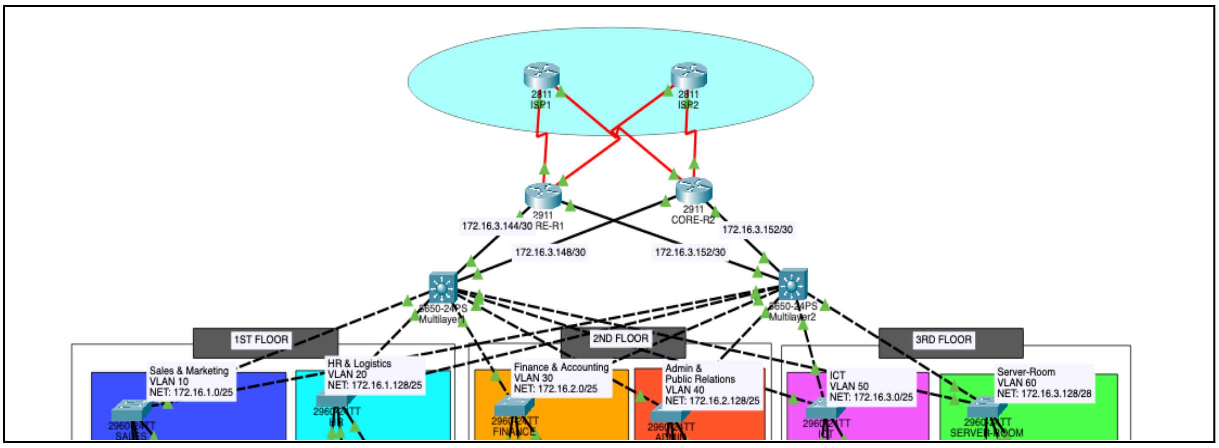
**1st Floor**

| Department | Network Address | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|
| Sales & Marketing | 172.16.1.0 | 255.255.255.128/25 | 172.16.1.1 to 172.16.1.126 | 172.16.1.127 |
| HR & Logistics | 172.16.1.128 | 255.255.255.128/25 | 172.16.1.129 to 172.16.1.254 | 172.16.1.255 |

**2nd Floor**

| Department | Network Address | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|
| Finance & Accounting | 172.16.2.0 | 255.255.255.128/25 | 172.16.2.1 to 172.16.2.126 | 172.16.2.127 |
| Admin & Public Relations | 172.16.2.128 | 255.255.255.128/25 | 172.16.2.129 to 172.16.2.254 | 172.16.2.255 |

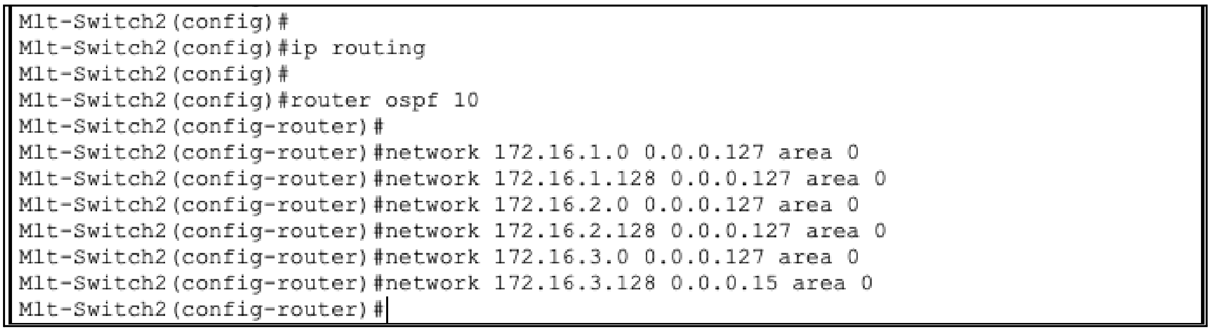
*Assigned IP addresses.*



## 5. OSPF Configuration (Routers & Switch 13)

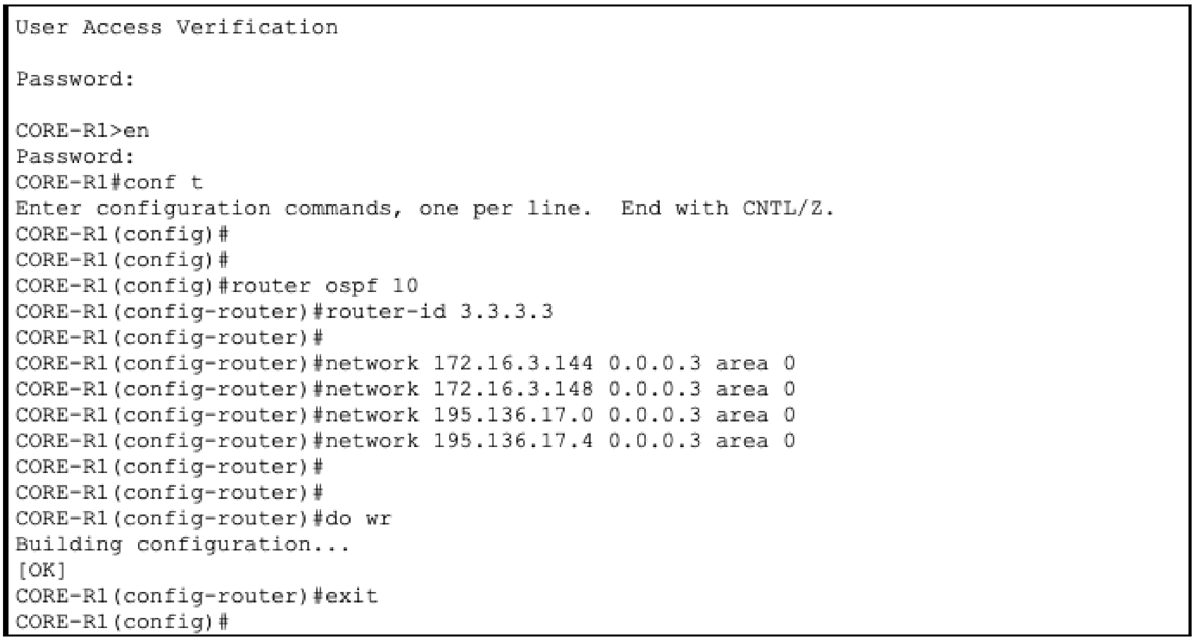
- Enable OSPF process
- Assign router IDs
- Advertise networks

*OSPF configuration on Mlt-Switch2.*



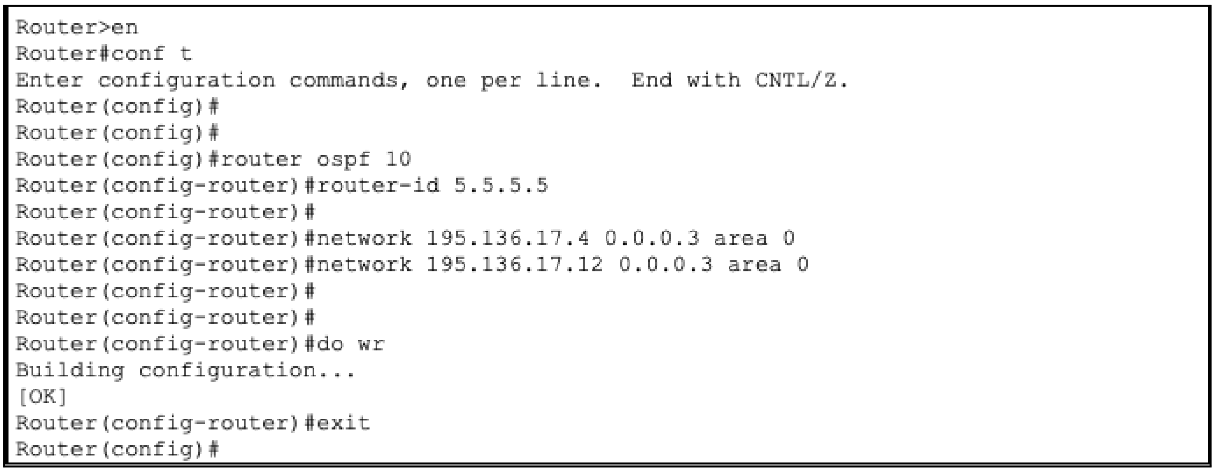
```
Mlt-Switch2(config)#
Mlt-Switch2(config)#ip routing
Mlt-Switch2(config)#
Mlt-Switch2(config)#router ospf 10
Mlt-Switch2(config-router)#
Mlt-Switch2(config-router)#network 172.16.1.0 0.0.0.127 area 0
Mlt-Switch2(config-router)#network 172.16.1.128 0.0.0.127 area 0
Mlt-Switch2(config-router)#network 172.16.2.0 0.0.0.127 area 0
Mlt-Switch2(config-router)#network 172.16.2.128 0.0.0.127 area 0
Mlt-Switch2(config-router)#network 172.16.3.0 0.0.0.127 area 0
Mlt-Switch2(config-router)#network 172.16.3.128 0.0.0.15 area 0
Mlt-Switch2(config-router)#
```

*OSPF configuration on CORE-R1.*



```
User Access Verification

Password:

CORE-R1>en
Password:
CORE-R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE-R1(config)#
CORE-R1(config)#
CORE-R1(config)#router ospf 10
CORE-R1(config-router)#router-id 3.3.3.3
CORE-R1(config-router)#
CORE-R1(config-router)#network 172.16.3.144 0.0.0.3 area 0
CORE-R1(config-router)#network 172.16.3.148 0.0.0.3 area 0
CORE-R1(config-router)#network 195.136.17.0 0.0.0.3 area 0
CORE-R1(config-router)#network 195.136.17.4 0.0.0.3 area 0
CORE-R1(config-router)#
CORE-R1(config-router)#
CORE-R1(config-router)#do wr
Building configuration...
[OK]
CORE-R1(config-router)#exit
CORE-R1(config)#
```

*OSPF configuration on Router..*



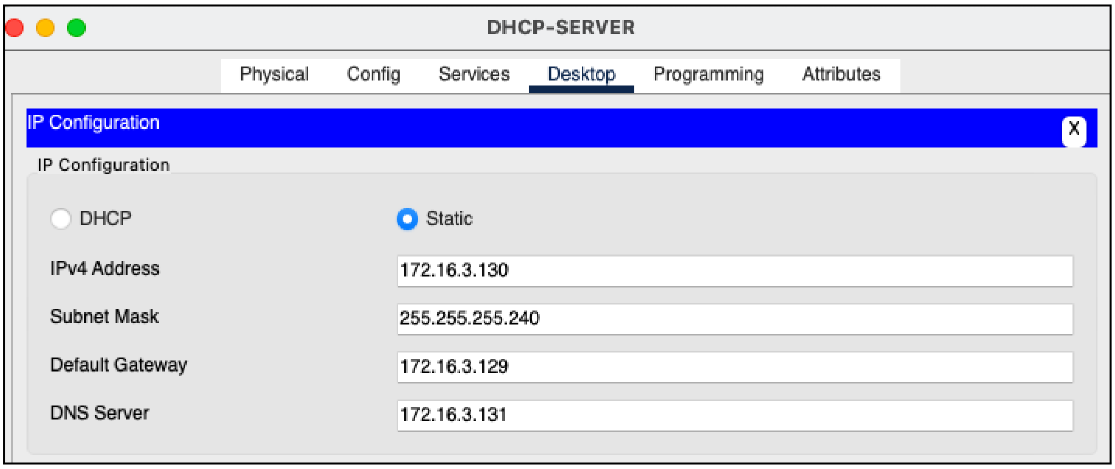
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#router ospf 10
Router(config-router)#router-id 5.5.5.5
Router(config-router)#
Router(config-router)#network 195.136.17.4 0.0.0.3 area 0
Router(config-router)#network 195.136.17.12 0.0.0.3 area 0
Router(config-router)#
Router(config-router)#
Router(config-router)#do wr
Building configuration...
[OK]
Router(config-router)#exit
Router(config)#
```

## 6. Static IP Addressing (Server Room Devices)

- Assign static IPs to servers (e.g., DNS, Web, DHCP)

**Figures:**

*DHCP server static IP configuration.*



IP Configuration

○ DHCP ● Static

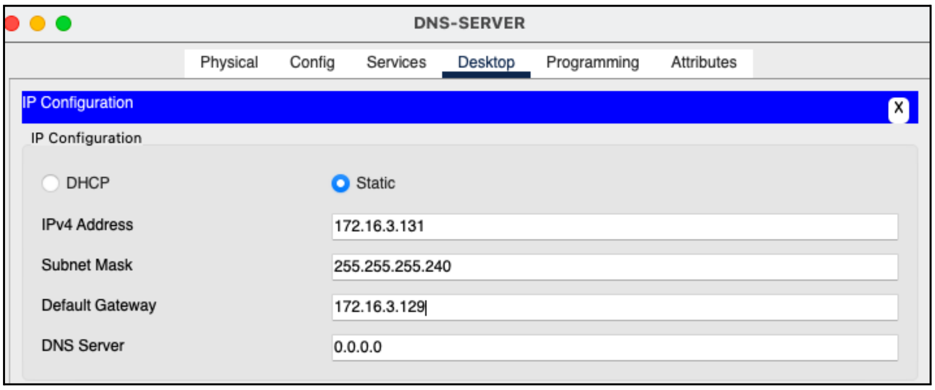
IPv4 Address 172.16.3.130

Subnet Mask 255.255.255.240

Default Gateway 172.16.3.129

DNS Server 172.16.3.131

*DNS server static IP configuration.*



IP Configuration

○ DHCP ● Static

IPv4 Address: 172.16.3.131

Subnet Mask: 255.255.255.240

Default Gateway: 172.16.3.129

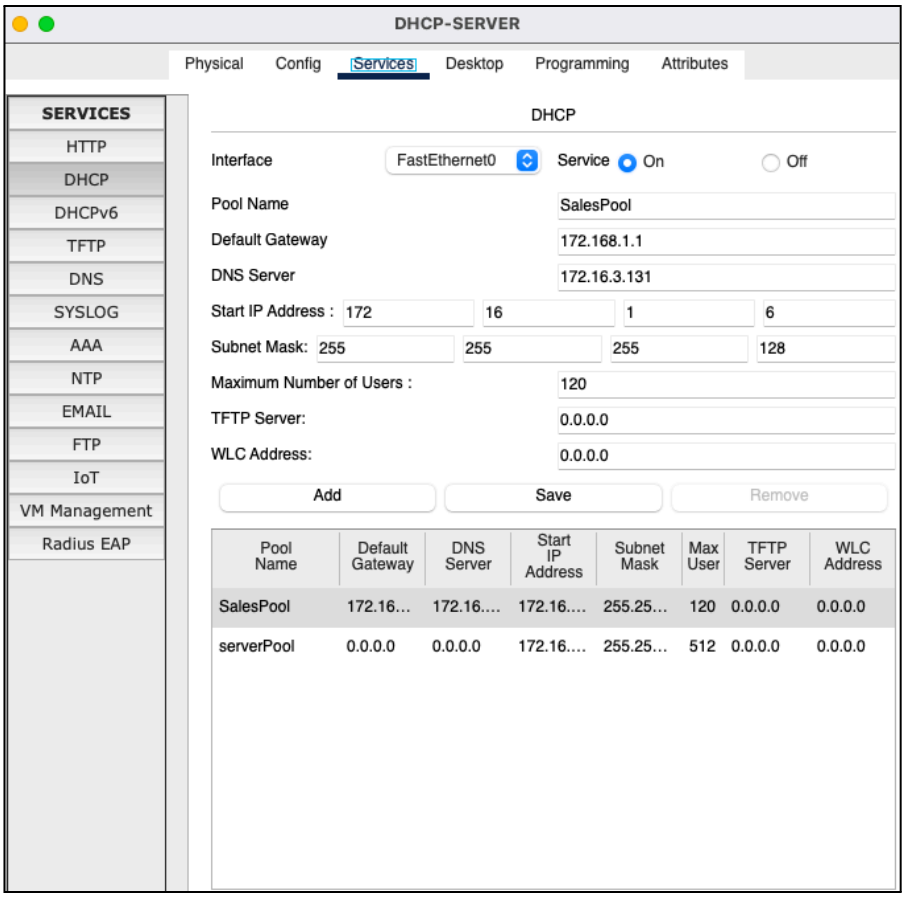
DNS Server: 0.0.0.0

# 7. DHCP Server Configuration

- Configure DHCP pools
- Exclude static IP addresses
- Apply helper address on Router/Switch 13

**Figures:**

*Configure DHCP pool for the **Sales** Department.*



DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: SalesPool

Default Gateway: 172.168.1.1

DNS Server: 172.16.3.131

Start IP Address : 172 16 1 6

Subnet Mask: 255 255 255 128

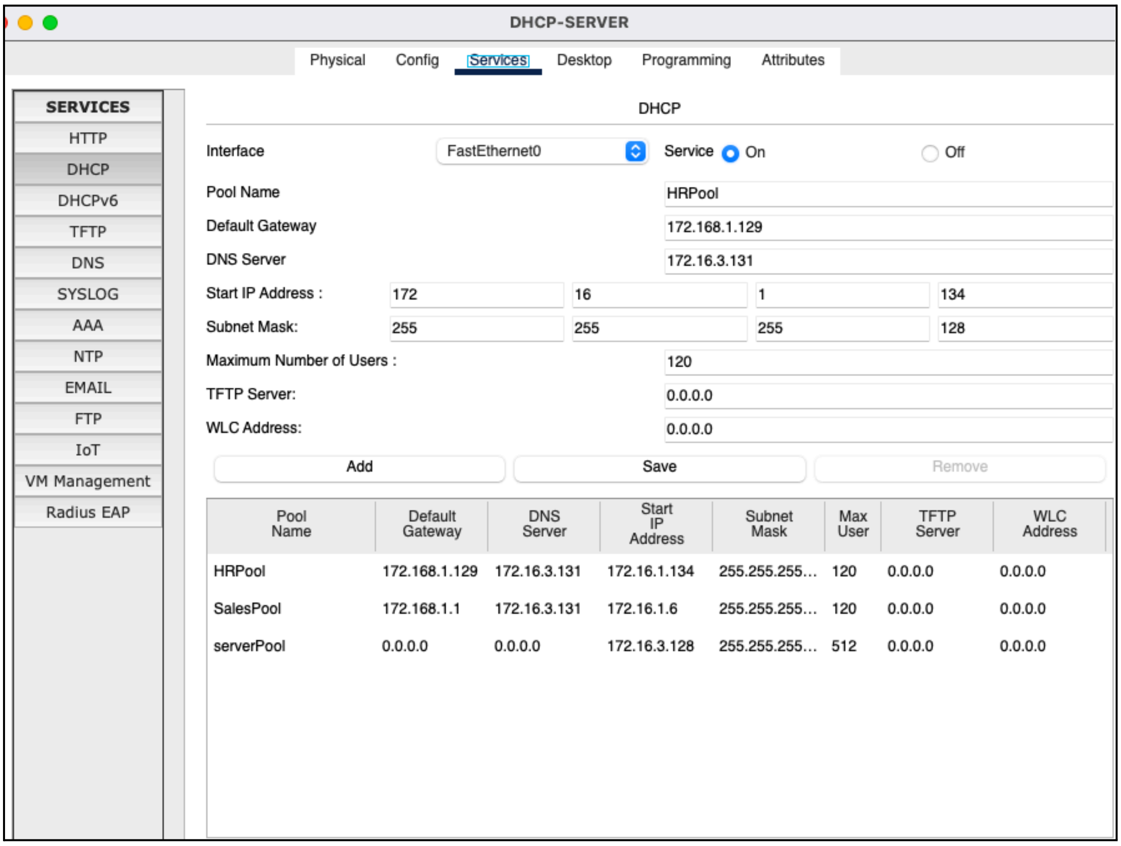
Maximum Number of Users : 120

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 |
|---|---|---|---|---|---|---|---|
| SalesPool | 172.16... | 172.16.... | 172.16.... | 255.25... | 120 | 0.0.0.0 | 0.0.0.0 |
| serverPool | 0.0.0.0 | 0.0.0.0 | 172.16.... | 255.25... | 512 | 0.0.0.0 | 0.0.0.0 |

*Configure DHCP pool for the* ***HR*** *Department.*



Interface: FastEthernet0

Service ● On ○ Off

Pool Name: HRPool

Default Gateway: 172.168.1.129

DNS Server: 172.16.3.131

Start IP Address : 172 16 1 134

Subnet Mask: 255 255 255 128

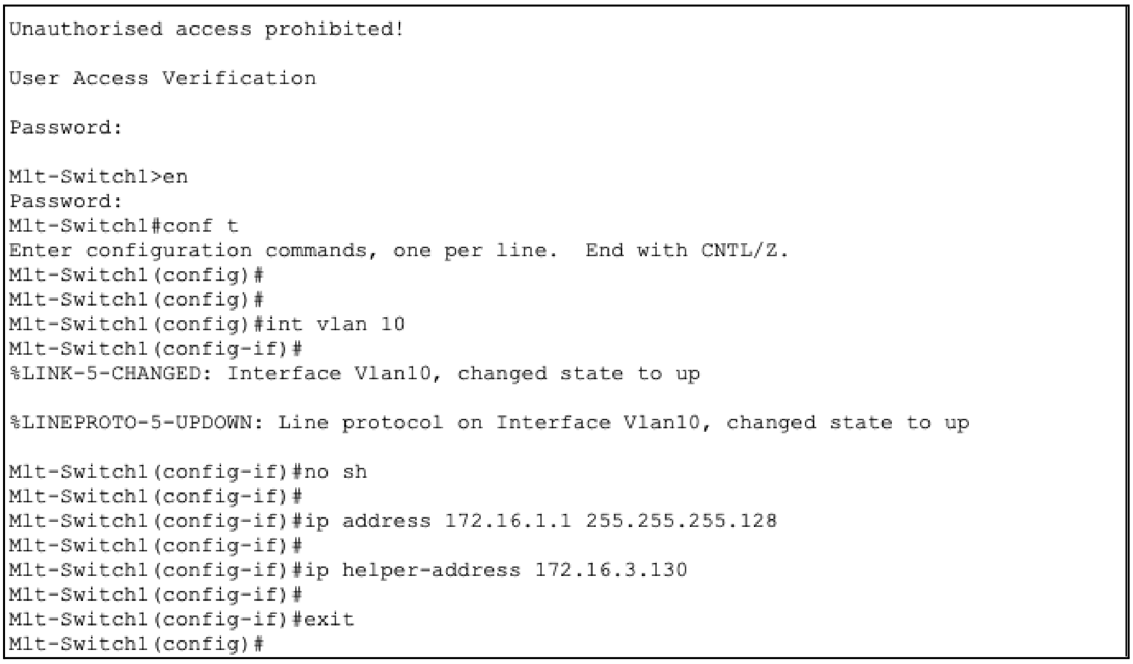
Maximum Number of Users : 120

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 |
|---|---|---|---|---|---|---|---|
| HRPool | 172.168.1.129 | 172.16.3.131 | 172.16.1.134 | 255.255.255... | 120 | 0.0.0.0 | 0.0.0.0 |
| SalesPool | 172.168.1.1 | 172.16.3.131 | 172.16.1.6 | 255.255.255... | 120 | 0.0.0.0 | 0.0.0.0 |
| serverPool | 0.0.0.0 | 0.0.0.0 | 172.16.3.128 | 255.255.255... | 512 | 0.0.0.0 | 0.0.0.0 |

*Apply helper address on Router/Switch 13*

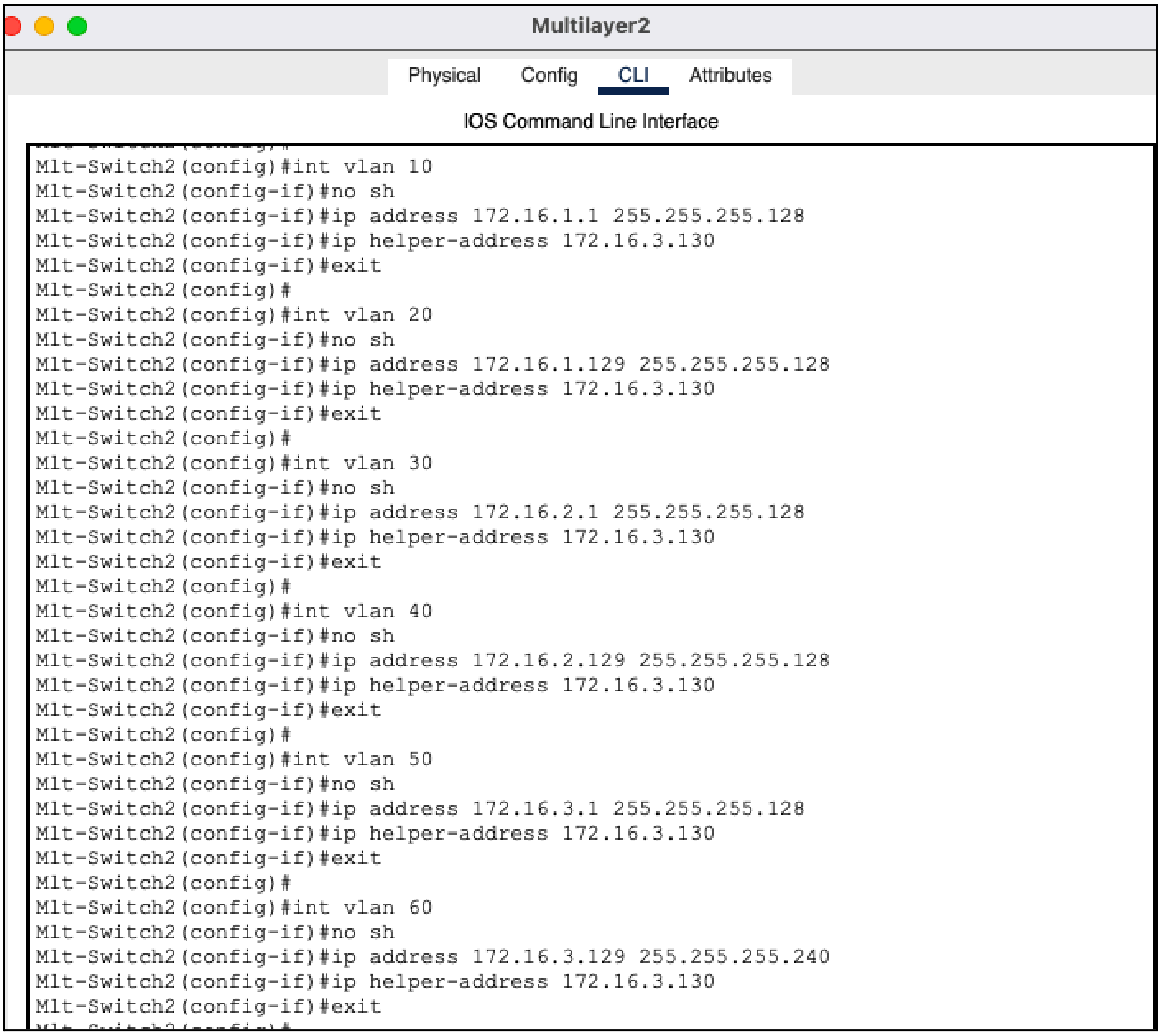


```
Unauthorised access prohibited!

User Access Verification

Password:

Mlt-Switch1>en
Password:
Mlt-Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Mlt-Switch1(config)#
Mlt-Switch1(config)#
Mlt-Switch1(config)#int vlan 10
Mlt-Switch1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

Mlt-Switch1(config-if)#no sh
Mlt-Switch1(config-if)#
Mlt-Switch1(config-if)#ip address 172.16.1.1 255.255.255.128
Mlt-Switch1(config-if)#
Mlt-Switch1(config-if)#ip helper-address 172.16.3.130
Mlt-Switch1(config-if)#
Mlt-Switch1(config-if)#exit
Mlt-Switch1(config)#
```

# 8. Inter-VLAN Routing (Switch 13)

- Enable routing on Switch 13
- Add ip helper-address for each VLAN

*Configure DHCP helper addresses on each VLAN.*



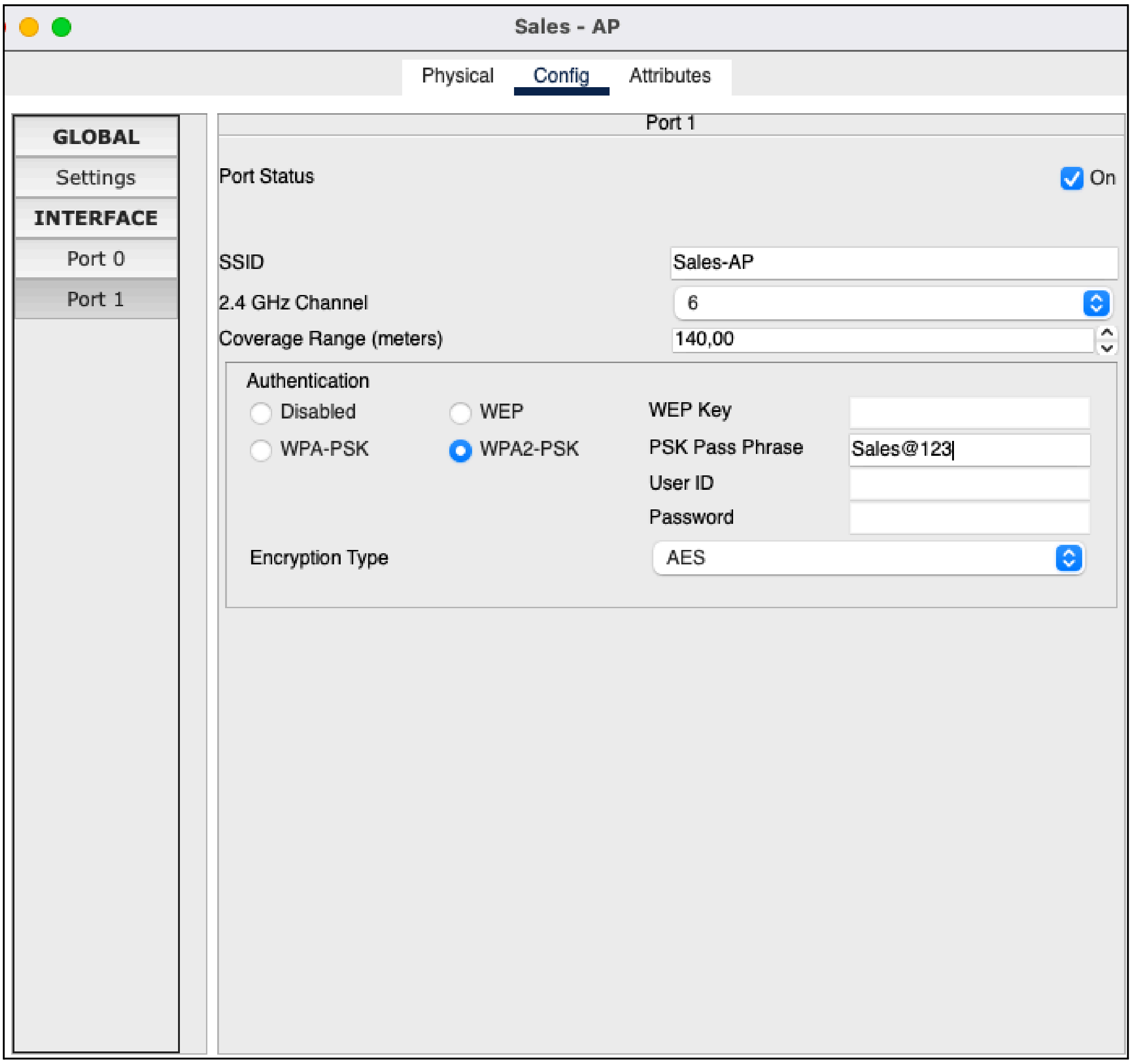
```
Mlt-Switch2(config)#
Mlt-Switch2(config)#int vlan 10
Mlt-Switch2(config-if)#no sh
Mlt-Switch2(config-if)#ip address 172.16.1.1 255.255.255.128
Mlt-Switch2(config-if)#ip helper-address 172.16.3.130
Mlt-Switch2(config-if)#exit
Mlt-Switch2(config)#
Mlt-Switch2(config)#int vlan 20
Mlt-Switch2(config-if)#no sh
Mlt-Switch2(config-if)#ip address 172.16.1.129 255.255.255.128
Mlt-Switch2(config-if)#ip helper-address 172.16.3.130
Mlt-Switch2(config-if)#exit
Mlt-Switch2(config)#
Mlt-Switch2(config)#int vlan 30
Mlt-Switch2(config-if)#no sh
Mlt-Switch2(config-if)#ip address 172.16.2.1 255.255.255.128
Mlt-Switch2(config-if)#ip helper-address 172.16.3.130
Mlt-Switch2(config-if)#exit
Mlt-Switch2(config)#
Mlt-Switch2(config)#int vlan 40
Mlt-Switch2(config-if)#no sh
Mlt-Switch2(config-if)#ip address 172.16.2.129 255.255.255.128
Mlt-Switch2(config-if)#ip helper-address 172.16.3.130
Mlt-Switch2(config-if)#exit
Mlt-Switch2(config)#
Mlt-Switch2(config)#int vlan 50
Mlt-Switch2(config-if)#no sh
Mlt-Switch2(config-if)#ip address 172.16.3.1 255.255.255.128
Mlt-Switch2(config-if)#ip helper-address 172.16.3.130
Mlt-Switch2(config-if)#exit
Mlt-Switch2(config)#
Mlt-Switch2(config)#int vlan 60
Mlt-Switch2(config-if)#no sh
Mlt-Switch2(config-if)#ip address 172.16.3.129 255.255.255.240
Mlt-Switch2(config-if)#ip helper-address 172.16.3.130
Mlt-Switch2(config-if)#exit
Mlt-Switch2(config)#
```

# 9. Wireless Network Setup

- Configure Wireless Router/Access Point
- Set SSID, WPA2 password
- Connect wireless devices

**Figures:**

*Configure Access Point with a suitable name and WPA2-PSK.*



Sales - AP

Port 1

Port Status ☑ On

SSID: Sales-AP

2.4 GHz Channel: 6

Coverage Range (meters): 140,00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

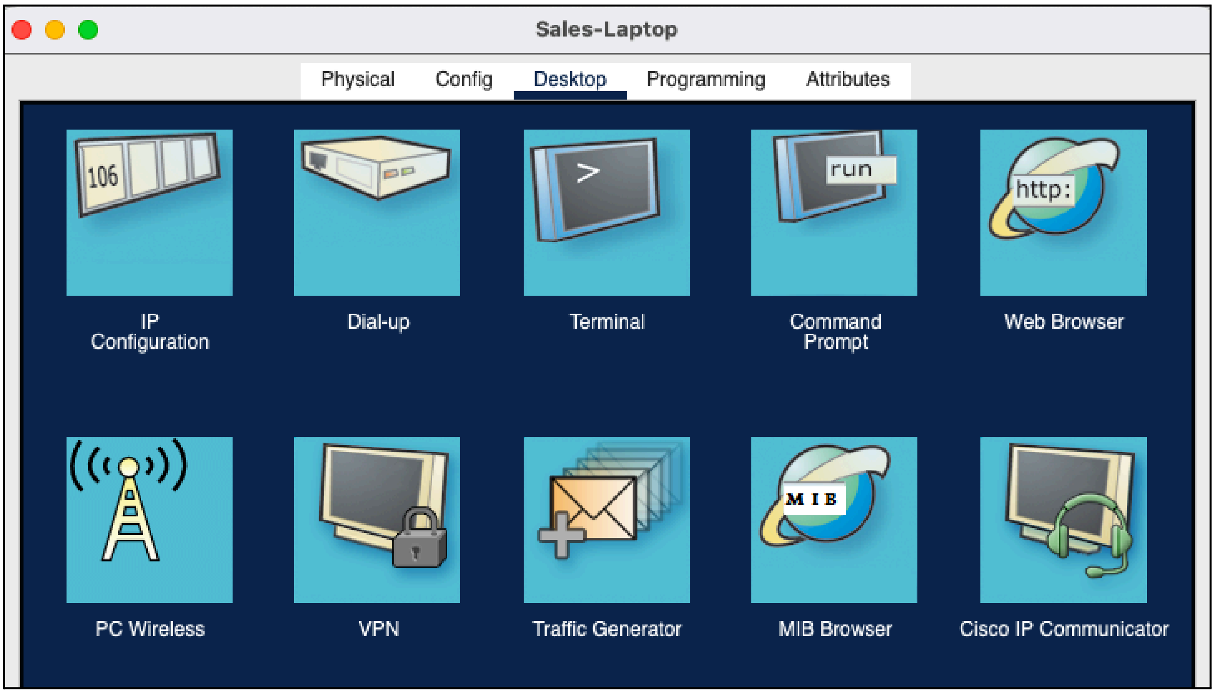
PSK Pass Phrase: Sales@123

User ID:

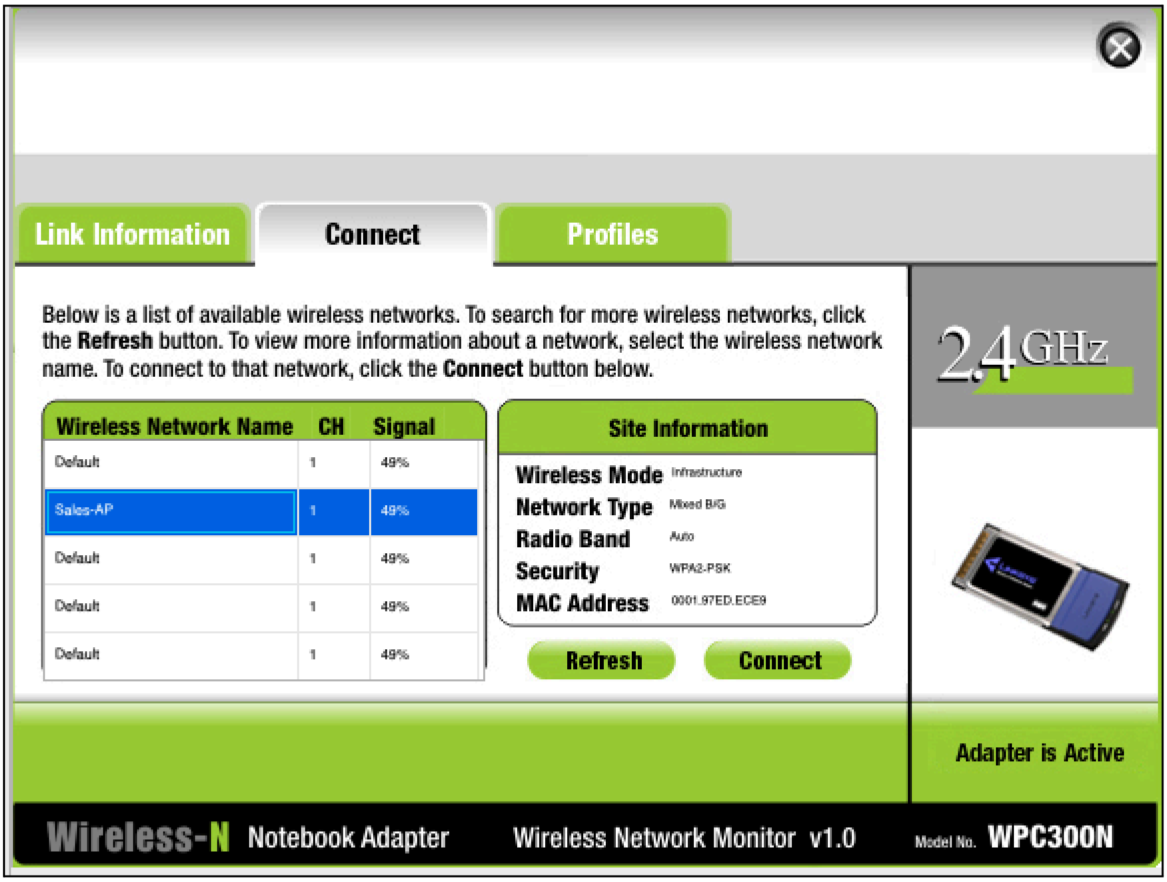
Password:

Encryption Type: AES

*Configure the Sales Department laptop for wireless connectivity.*



*Refresh and click on the suitable wireless network name.*



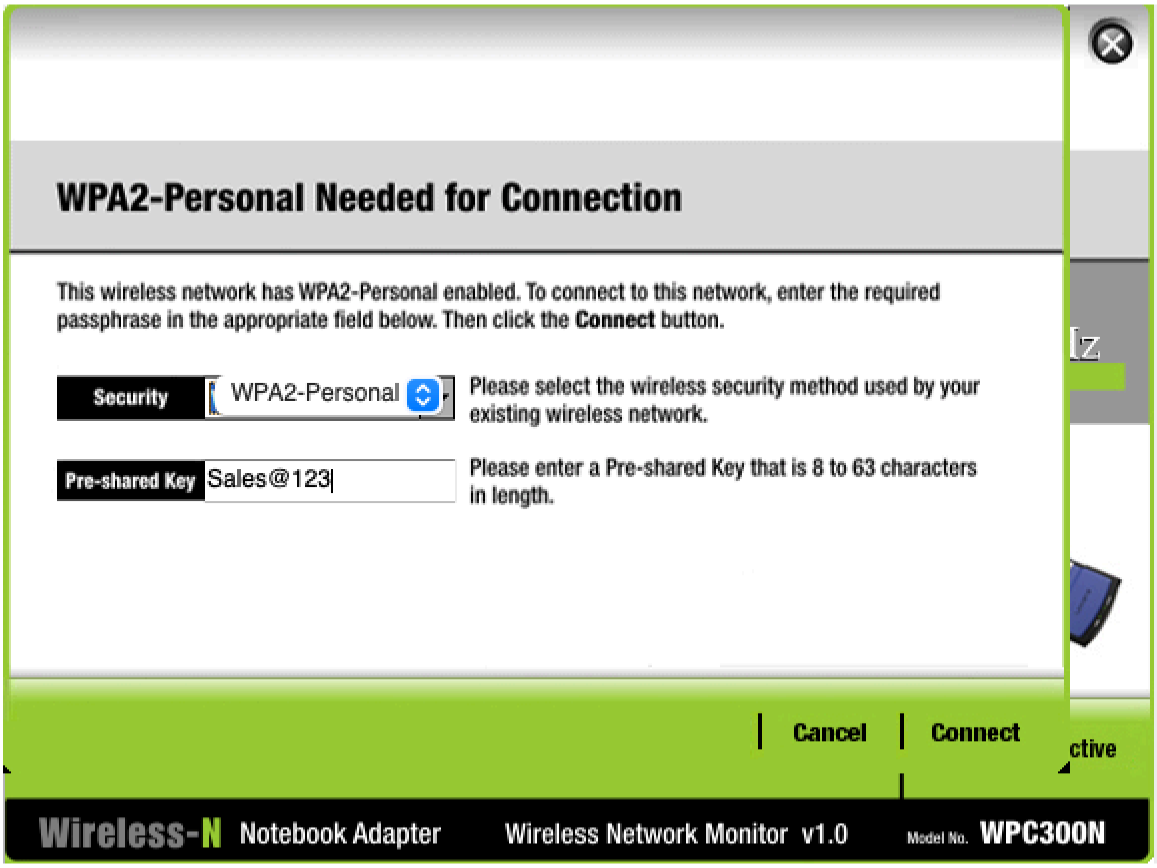
Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

| Wireless Network Name | CH | Signal |
|---|---|---|
| Default | 1 | 49% |
| Sales-AP | 1 | 49% |
| Default | 1 | 49% |
| Default | 1 | 49% |
| Default | 1 | 49% |

Site Information

Wireless Mode Infrastructure
Network Type Mixed B/G
Radio Band Auto
Security WPA2-PSK
MAC Address 0001.97ED.ECE9

*Enter the security type and password.*

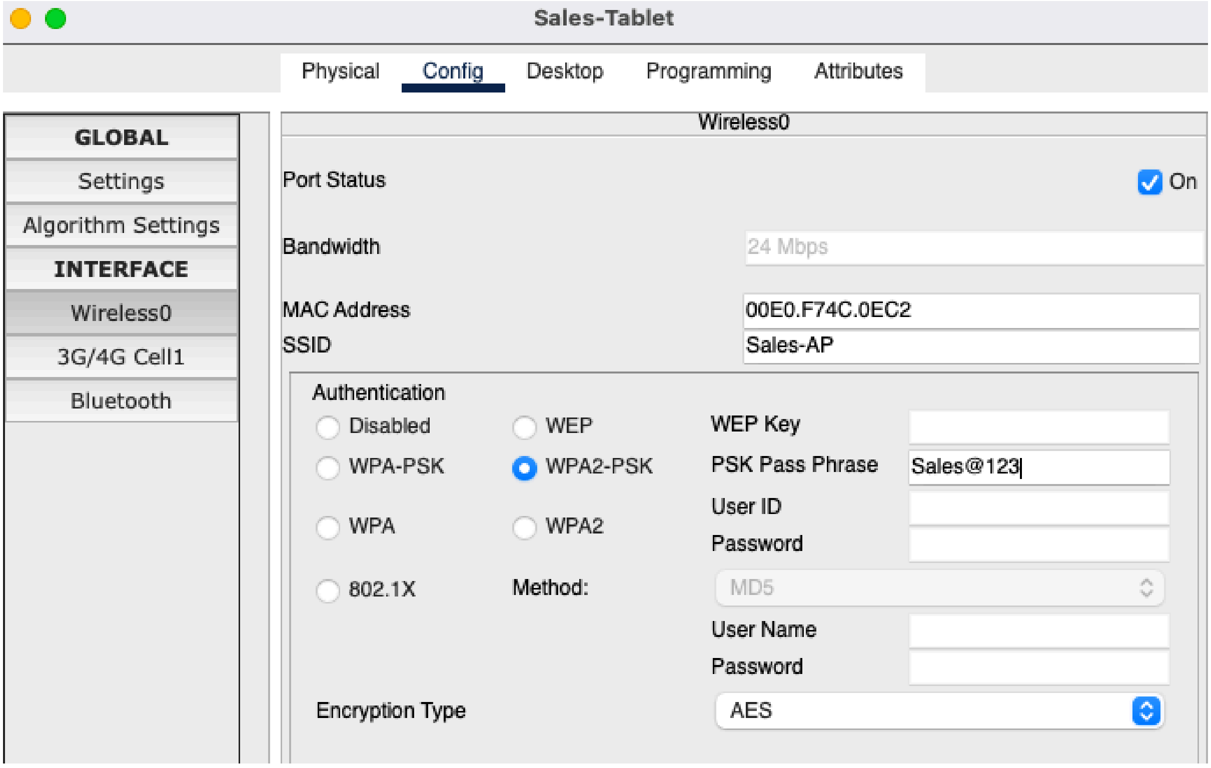


## WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

| | | |
|---|---|---|
| Security | WPA2-Personal | Please select the wireless security method used by your existing wireless network. |
| Pre-shared Key | Sales@123 | Please enter a Pre-shared Key that is 8 to 63 characters in length. |

*Configure the Sales Department tablet for wireless connectivity.*



Wireless0

Port Status ☑ On

Bandwidth: 24 Mbps

MAC Address: 00E0.F74C.0EC2

SSID: Sales-AP

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

○ WPA ○ WPA2

○ 802.1X Method: MD5

WEP Key:

PSK Pass Phrase: Sales@123

User ID:

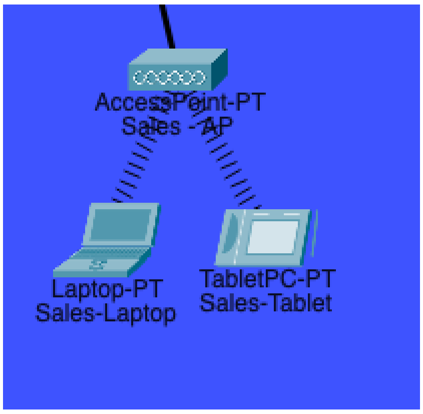
Password:

User Name:

Password:

Encryption Type: AES

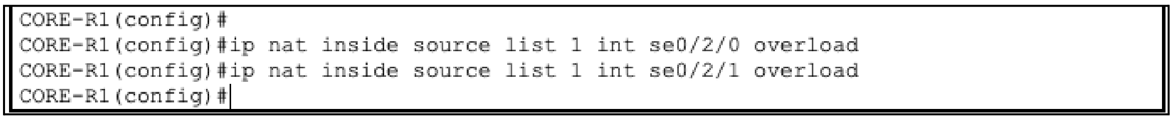
*Connection established.*



## 10. Port Address Translation (PAT) + ACL

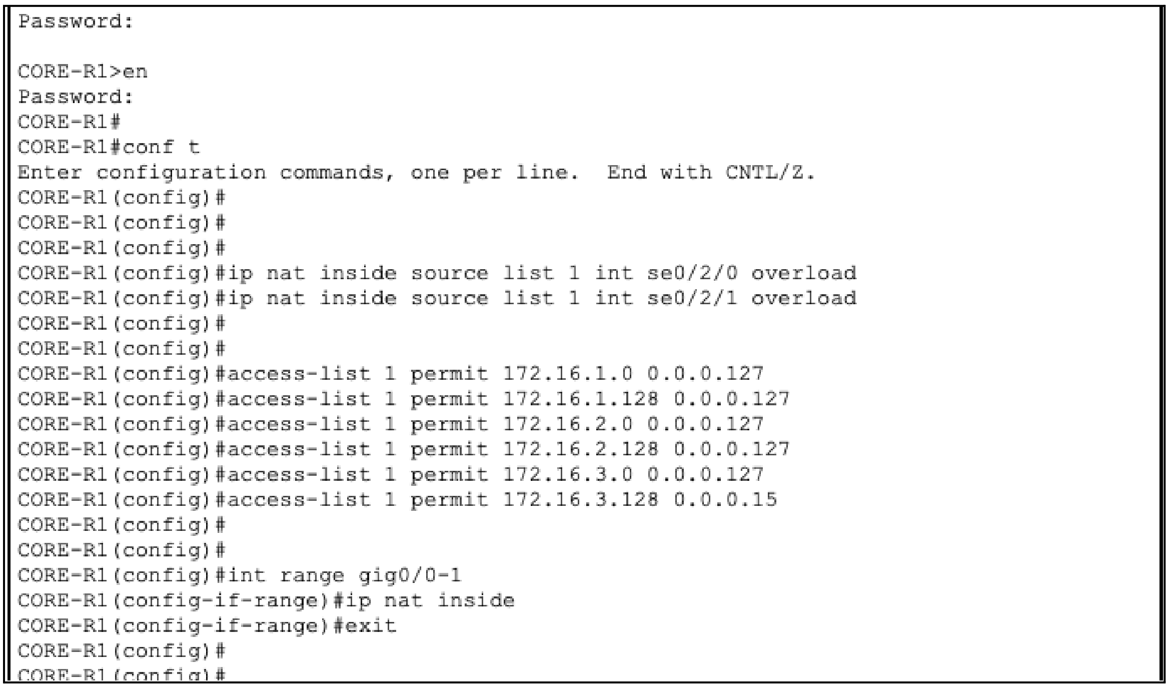
- Configure NAT overload (PAT) on edge router
- Create ACL to allow only authorised subnets to access the internet

*Network Address Translation (NAT) overload.*



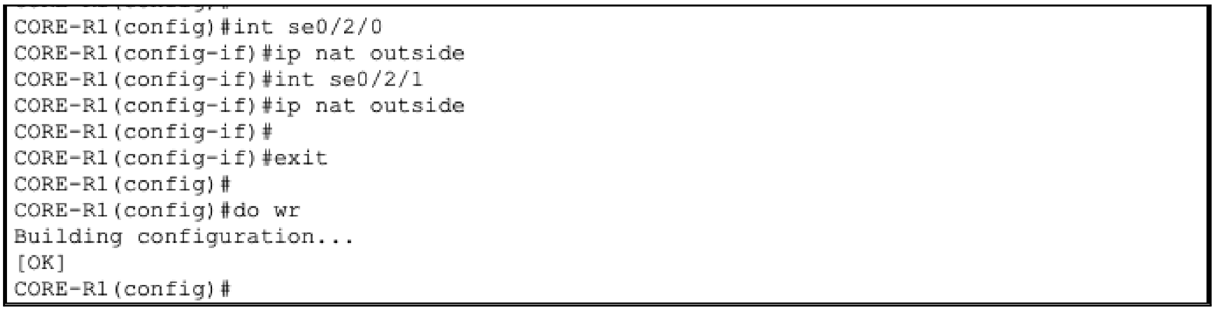
```
CORE-R1(config)#
CORE-R1(config)#ip nat inside source list 1 int se0/2/0 overload
CORE-R1(config)#ip nat inside source list 1 int se0/2/1 overload
CORE-R1(config)#
```

*Access Control List (ACL) configuration.*



```
Password:

CORE-R1>en
Password:
CORE-R1#
CORE-R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE-R1(config)#
CORE-R1(config)#
CORE-R1(config)#
CORE-R1(config)#ip nat inside source list 1 int se0/2/0 overload
CORE-R1(config)#ip nat inside source list 1 int se0/2/1 overload
CORE-R1(config)#
CORE-R1(config)#
CORE-R1(config)#access-list 1 permit 172.16.1.0 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.1.128 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.2.0 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.2.128 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.3.0 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.3.128 0.0.0.15
CORE-R1(config)#
CORE-R1(config)#
CORE-R1(config)#int range gig0/0-1
CORE-R1(config-if-range)#ip nat inside
CORE-R1(config-if-range)#exit
CORE-R1(config)#
CORE-R1(config)#
```

*Cont.*

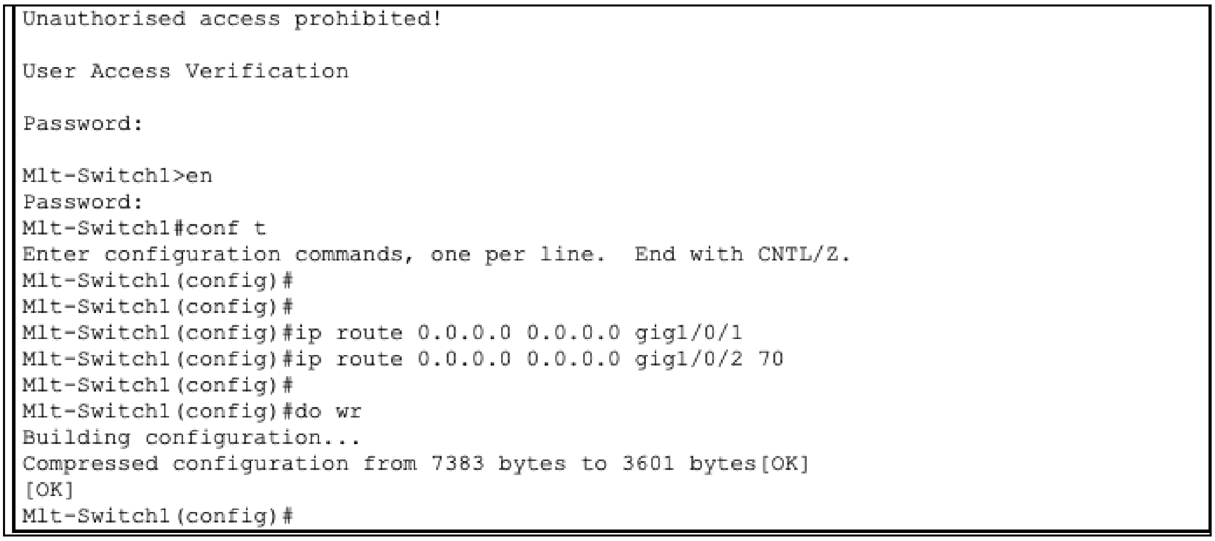


```
CORE-R1(config)#int se0/2/0
CORE-R1(config-if)#ip nat outside
CORE-R1(config-if)#int se0/2/1
CORE-R1(config-if)#ip nat outside
CORE-R1(config-if)#
CORE-R1(config-if)#exit
CORE-R1(config)#
CORE-R1(config)#do wr
Building configuration...
[OK]
CORE-R1(config)#
```

## 11. Default Static Route

- Configure default route to ISP router

*Default Static Route configuration.*



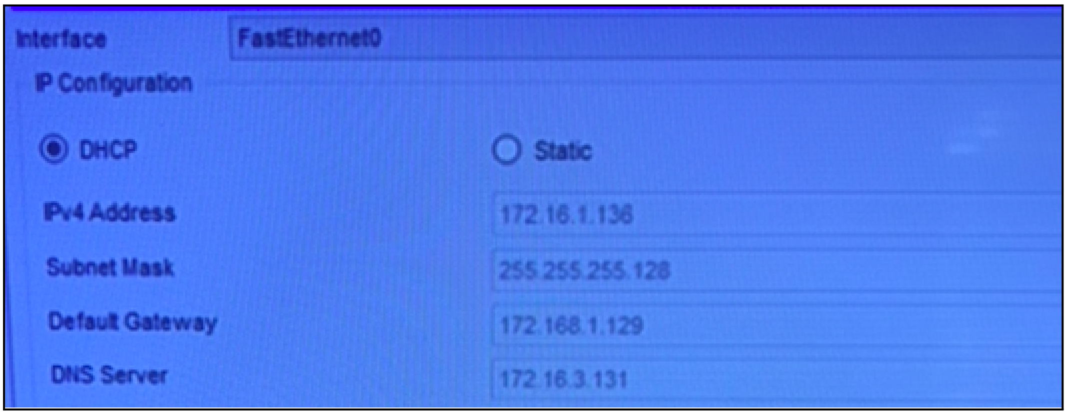
```
Unauthorised access prohibited!

User Access Verification

Password:

Mlt-Switch1>en
Password:
Mlt-Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Mlt-Switch1(config)#
Mlt-Switch1(config)#
Mlt-Switch1(config)#ip route 0.0.0.0 0.0.0.0 gig1/0/1
Mlt-Switch1(config)#ip route 0.0.0.0 0.0.0.0 gig1/0/2 70
Mlt-Switch1(config)#
Mlt-Switch1(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Mlt-Switch1(config)#
```

## 12. Verification & Testing

- **Ping test:** PCs to PCs, PCs to Servers, PCs to Internet
- **VLAN test:** Devices in the same VLAN should communicate, different VLANs only via routing
- **DHCP test:** End devices should get IPs dynamically
- **SSH test:** Remote login to router/switch
- **Wireless test:** Wireless PC gets IP + internet access

**Figures:**

*DHCP on HR-Laptop.*



Interface FastEthernet0

IP Configuration

● DHCP ○ Static

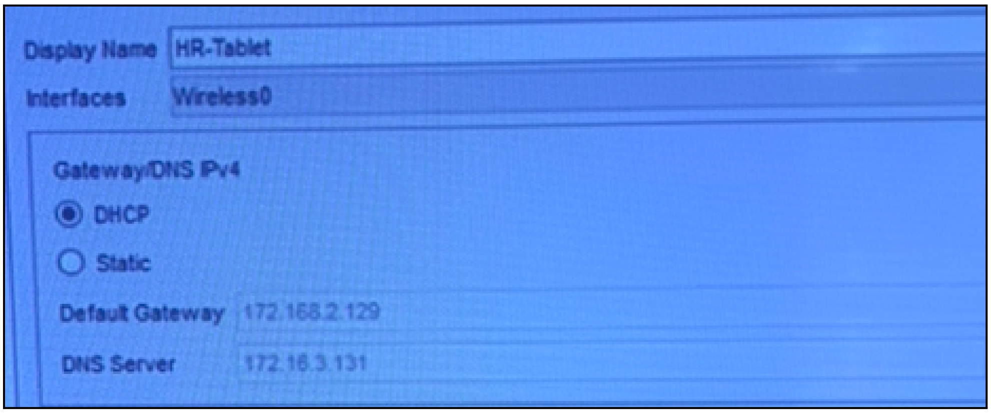
IPv4 Address 172.16.1.136

Subnet Mask 255.255.255.128

Default Gateway 172.168.1.129

DNS Server 172.16.3.131

*DHCP on HR-Tablet.*



Display Name HR-Tablet

Interfaces Wireless0

Gateway/DNS IPv4

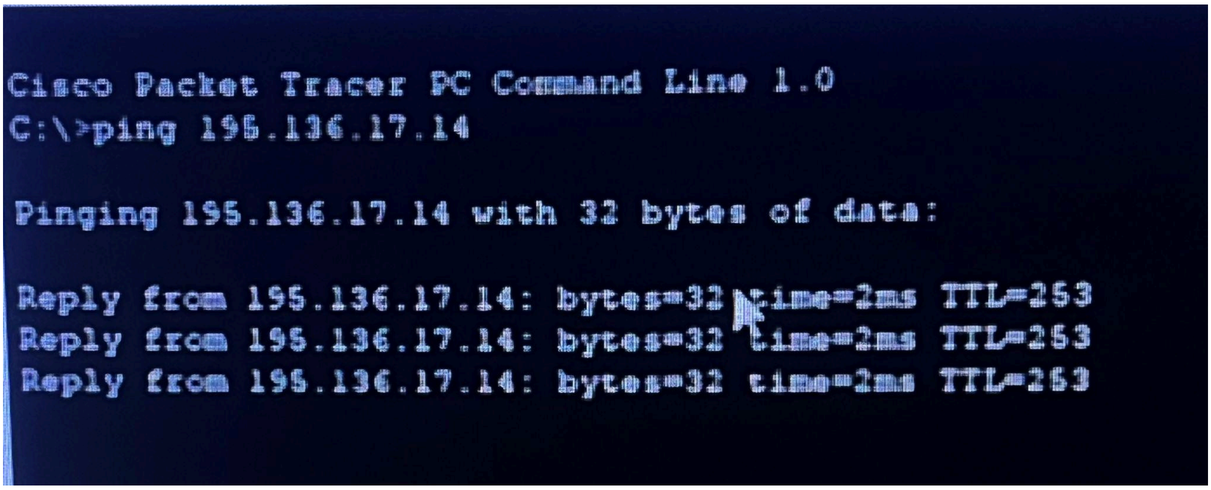
● DHCP

○ Static

Default Gateway 172.168.2.129

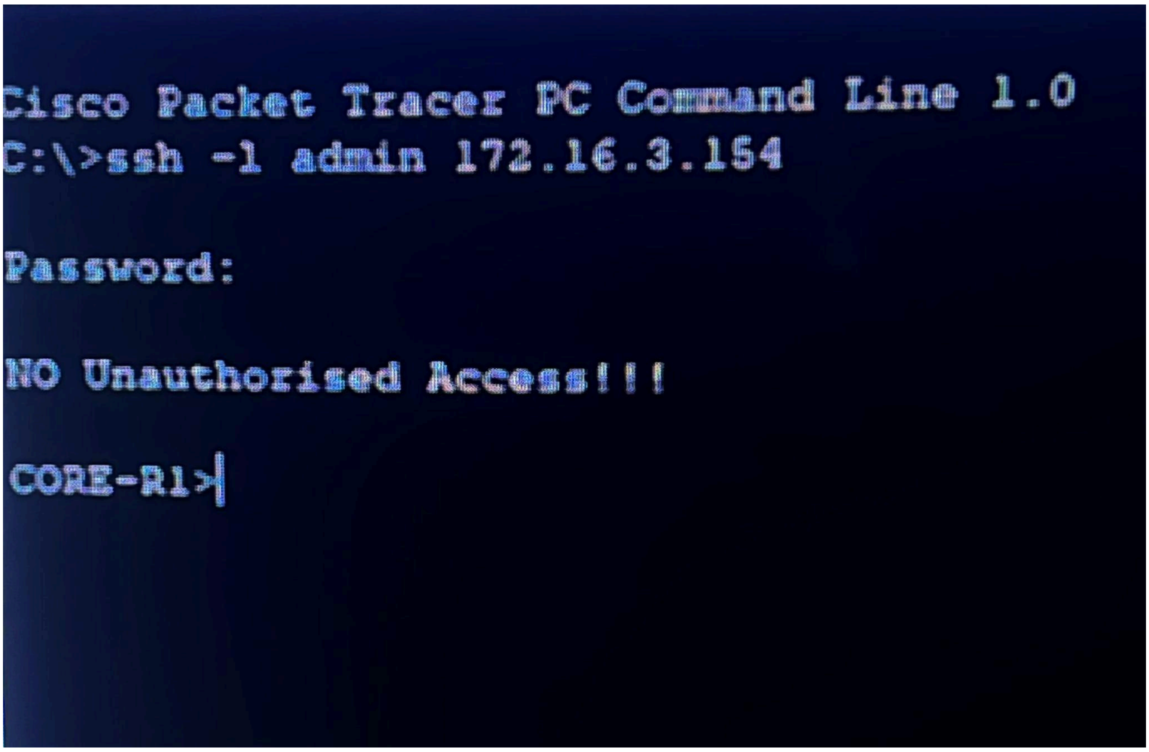
DNS Server 172.16.3.131

*Pinging works.*



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 195.136.17.14

Pinging 195.136.17.14 with 32 bytes of data:

Reply from 195.136.17.14: bytes=32 time=2ms TTL=253
Reply from 195.136.17.14: bytes=32 time=2ms TTL=253
Reply from 195.136.17.14: bytes=32 time=2ms TTL=253
```

*SSH working.*



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 172.16.3.154

Password:

NO Unauthorised Access!!!

CORE-R1>
```

---

## Final Thoughts

This project successfully configured a secure, segmented, and fully connected enterprise network. All devices can communicate across VLANs, internet access is controlled, and essential services (DHCP, DNS, NAT, wireless) are operational.