

# **Network Topology and Implementation for Tech Zolutions Inc**

Created By: Jordan Furtado

## Contents

WM9PD-15 Network Security PMA .....	<b>Error! Bookmark not defined.</b>
1. Executive Summary .....	3
2. Task 1: Network Design and Configuration .....	4
2.1 MS Visio Basic Network Layout .....	4
2.2 Network Topology Design.....	5
2.3 IP Addressing and Subnetting.....	5
2.4 VLAN Configuration .....	6
2.5 DHCP Configuration .....	10
2.6 Routing Configuration.....	13
2.7 Wireless Network Configuration.....	13
2.8 Verification.....	15
3. Task 2: Security and Zones of Trust .....	17
3.1 Security Measures on Network Devices .....	17
3.2 Zones of Trust.....	18
3.3 Zone-Policy Firewall (ZPF) Configuration.....	22
3.4 Access Control Lists (ACLs) .....	28
4. Task 3: Advanced Security Configuration.....	29
4.1 Site-to-Site VPN Configuration .....	29
4.2 AAA Server Configuration.....	33
5. Conclusion.....	35

# 1. Executive Summary

This report presents the Network Security Design and Implementation for Tech Zolutions Inc., addressing their need for a secure, scalable, and efficient network infrastructure. The project is divided into three key tasks: Network Design and Configuration, Security and Zones of Trust, and Advanced Security Implementation.

## **Network Design and Configuration**

A router-on-a-stick topology was implemented using a Internal Router, connected to a core switch that distributes network traffic among department-specific Layer 2 switches. VLANs were assigned for each department to improve network segmentation, reduce congestion, and enhance security. The IP addressing scheme is based on the 172.16.10.0/24 subnet, with tailored subnetting for departments.

A DHCP server in the server room dynamically allocates IP addresses, while inter-VLAN routing is enabled. Wireless connectivity was established using WPA2-PSK authentication, ensuring secure departmental SSIDs. Verification tests confirmed seamless inter-VLAN communication, proper DHCP assignments, and access to critical services like email and web servers.

## **Security and Zones of Trust**

Security measures were implemented through password-protected device access, AAA authentication, and encryption. Zones of Trust were established, categorizing the network into Internal, DMZ, and External zones to minimize security risks. The DMZ hosts public-facing services, including email and web servers, while the internal network remains isolated from direct external threats.

A Zone-Based Firewall (ZBF) was configured on Router1, with ACLs controlling traffic between security zones. Stateful inspection ensures only legitimate traffic is allowed, preventing unauthorized access. The firewall rules were validated, confirming that only permitted services, such as HTTP, HTTPS, DNS, and ICMP, function correctly while blocking unauthorized access attempts.

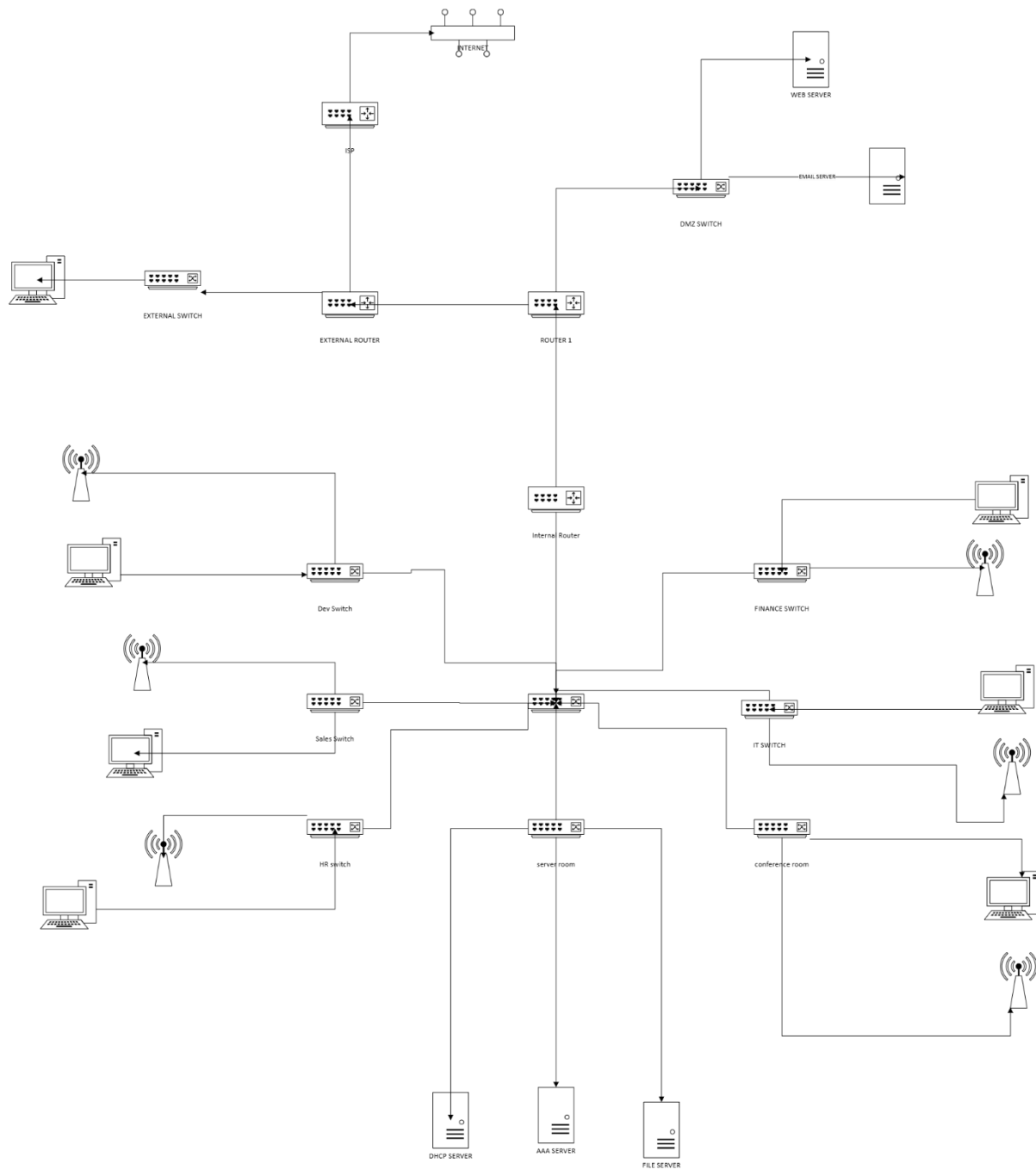
## **Advanced Security Implementation**

A site-to-site VPN was deployed between the External Router and Main Router using IPsec encryption to secure remote branch communications. The VPN utilizes AES-256 encryption, pre-shared keys, and ESP encapsulation, ensuring data confidentiality and integrity. A Zone-Based Firewall exception was created for VPN traffic, enabling encrypted communication while maintaining security.

A AAA server (TACACS+) was integrated for centralized authentication, authorization, and accounting. User roles and privileges were assigned, restricting unauthorized access. Security verification tests confirmed successful authentication via AAA and secure access to internal services over VPN.

## 2. Task 1: Network Design and Configuration

### 2.1 MS Visio Basic Network Layout



## 2.2 Network Topology Design

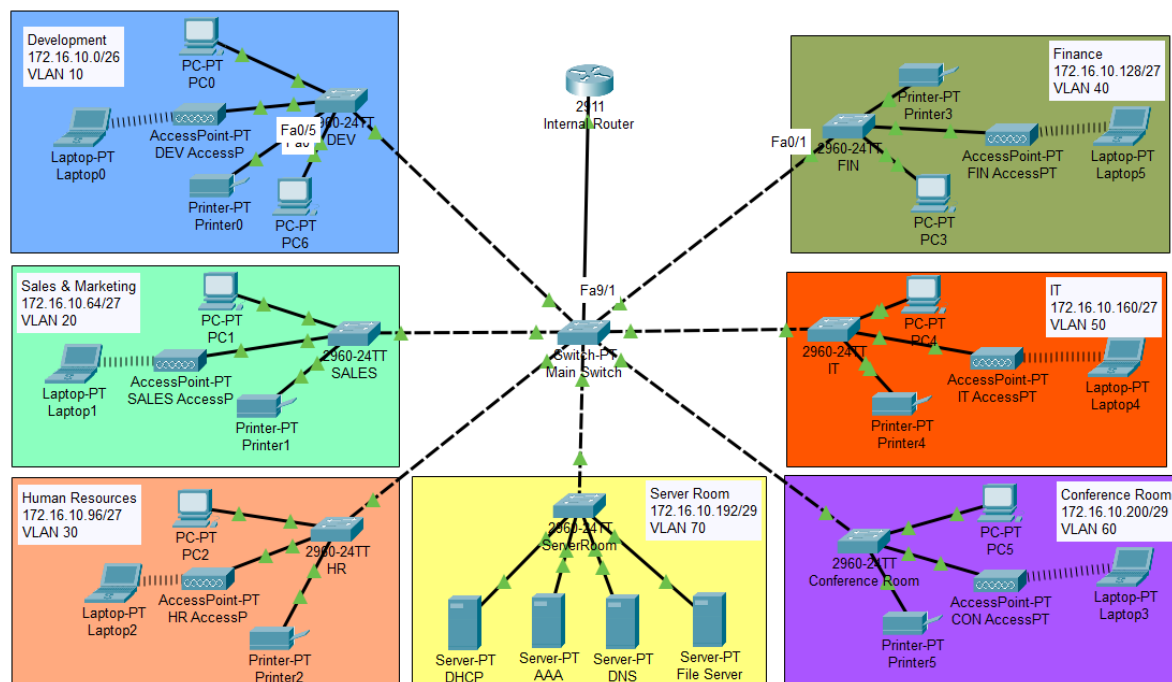


Figure 1 Task 1 diagram

2911 Internal Router with a router-on-a-stick configuration for inter-VLAN routing, reducing hardware costs while centralizing network control. A core switch connects all department switches, ensuring efficient communication. Each department has a Layer 2 switch (Cisco 2960-24TT) to segment traffic, reducing congestion and enhancing security.

I implemented VLANs to isolate departments, preventing unnecessary traffic and ensuring only authorized access. The server room (VLAN 70) is separate to protect critical services like DHCP, AAA, DNS, and file storage.

Wireless connectivity is provided via access points in each department, ensuring flexibility for mobile users. This design optimizes performance, enhances security, and allows for future scalability.

## 2.3 IP Addressing and Subnetting

- the base address is **172.16.10.0/24**.

Department	Employees	Subnet Mask	Usable IP Range	Broadcast Address	Default Gateway
<b>Development</b>	50	/26 (255.255.255.192)	172.16.10.1 - 172.16.10.62	172.16.10.63	172.16.10.1
<b>Sales &amp; Marketing</b>	30	/27 (255.255.255.224)	172.16.10.64 - 172.16.10.94	172.16.10.95	172.16.10.65

<b>Human Resources</b>	25	/27 (255.255.255.224)	172.16.10.96 - 172.16.10.126	172.16.10.127	172.16.10.97
<b>Finance</b>	25	/27 (255.255.255.224)	172.16.10.128 - 172.16.10.158	172.16.10.159	172.16.10.129
<b>IT</b>	20	/27 (255.255.255.224)	172.16.10.160 - 172.16.10.190	172.16.10.191	172.16.10.161
<b>Server Room</b>	4 servers	/29 (255.255.255.248)	172.16.10.192 - 172.16.10.198	172.16.10.199	172.16.10.193
<b>Conference Room</b>	5 devices	/29 (255.255.255.248)	172.16.10.200 - 172.16.10.206	172.16.10.207	172.16.10.201

## 2.4 VLAN Configuration

To enable inter-VLAN communication, I configured subinterfaces on the main router (2911 Internal Router). Since this is a router-on-a-stick setup, a single physical interface handles multiple VLANs through 802.1Q trunking. Each VLAN requires a subinterface with an assigned IP address (default gateway) for routing.

### VLAN Table:

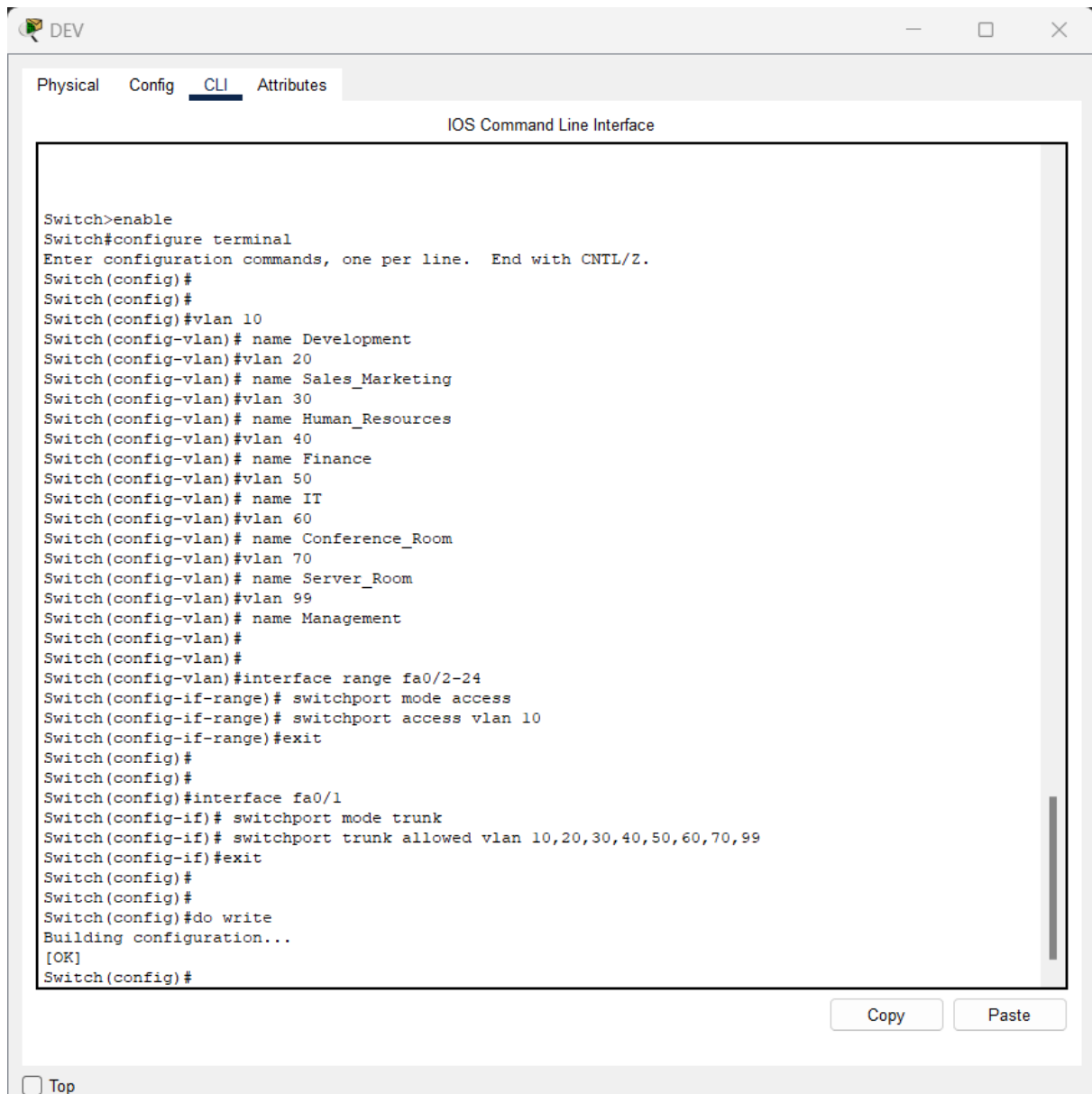
Subinterface	VLAN ID	Purpose	IP Address (Default Gateway)
G0/0.10	10	Development	172.16.10.1
G0/0.20	20	Sales	172.16.10.65
G0/0.30	30	HR	172.16.10.97
G0/0.40	40	Finance	172.16.10.129
G0/0.50	50	IT	172.16.10.161
G0/0.60	60	Conference	172.16.10.201
G0/0.70	70	Server Room	172.16.10.193

### Justification for VLAN & Device Configuration

- **Traffic Isolation:** VLANs prevent unnecessary interdepartmental traffic.
- **Controlled Access:** Only essential communication between VLANs is allowed.

- **Scalability:** New departments or subnets can be added without disrupting the entire network.

### Department Switch Configuration (Example: Development Room)



The screenshot shows a network configuration window titled 'DEV' with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the 'IOS Command Line Interface'. The terminal shows the following commands and prompts:

```

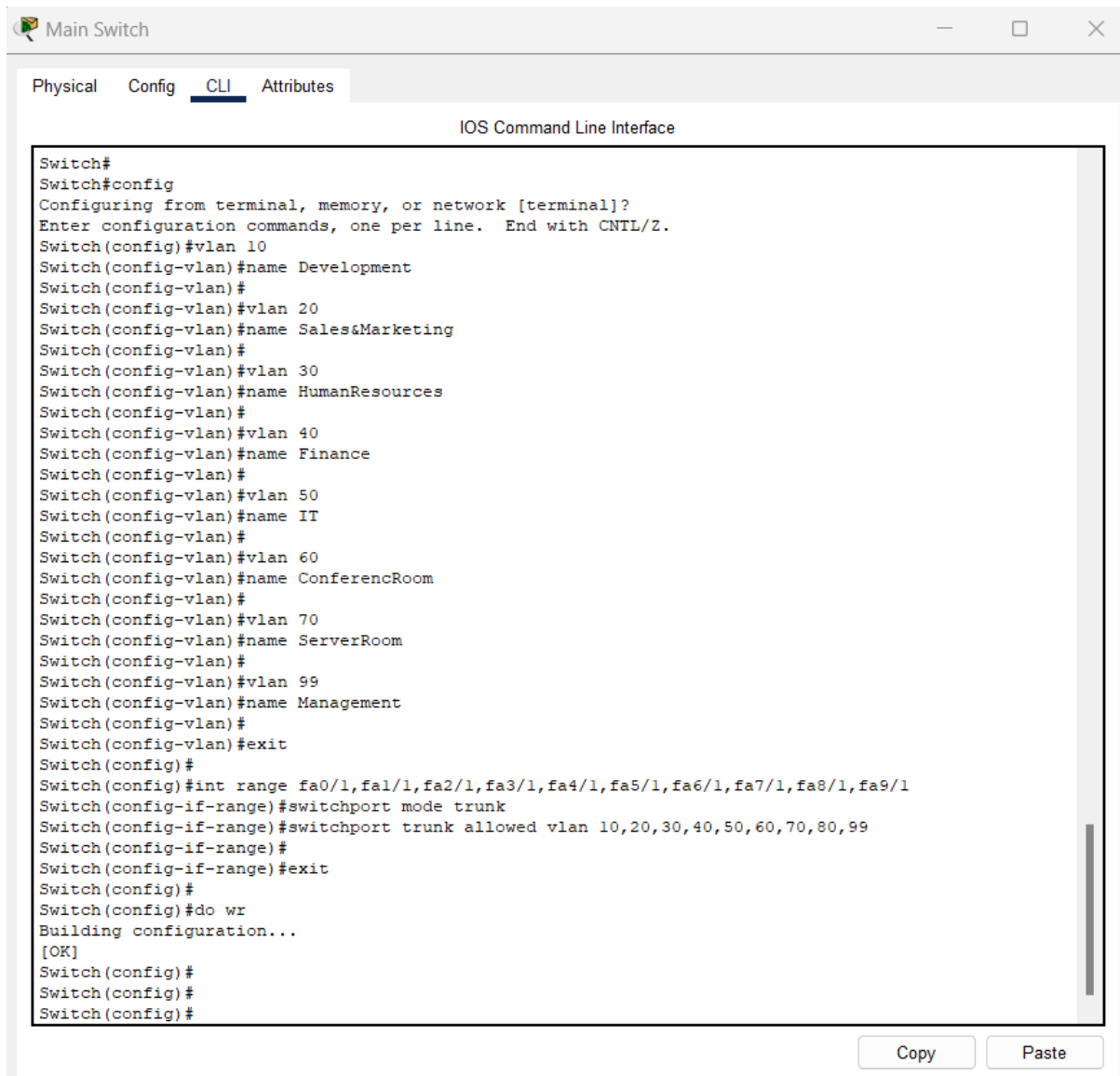
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)# name Development
Switch(config-vlan)#vlan 20
Switch(config-vlan)# name Sales_Marketing
Switch(config-vlan)#vlan 30
Switch(config-vlan)# name Human_Resources
Switch(config-vlan)#vlan 40
Switch(config-vlan)# name Finance
Switch(config-vlan)#vlan 50
Switch(config-vlan)# name IT
Switch(config-vlan)#vlan 60
Switch(config-vlan)# name Conference_Room
Switch(config-vlan)#vlan 70
Switch(config-vlan)# name Server_Room
Switch(config-vlan)#vlan 99
Switch(config-vlan)# name Management
Switch(config-vlan)#
Switch(config-vlan)#
Switch(config-vlan)#interface range fa0/2-24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface fa0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70,99
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#do write
Building configuration...
[OK]
Switch(config)#
  
```

At the bottom of the window, there is a 'Top' button and a scroll bar. Below the terminal area are 'Copy' and 'Paste' buttons.

Figure 2Dept-switch vlan-config

The switch is configured with multiple VLANs (10-70 and 99 for management) to separate network traffic by department. Fa0/2-24 are configured as access ports assigned to VLAN 10, ensuring that only Development devices connect to this VLAN. Fa0/1 is set as a trunk port, allowing traffic from multiple VLANs to communicate with the core switch. These commands need to be repeated for the other 6 department switches changing the device access to the respective VLAN id

### Multilayer Switch (Core Switch) Configuration



The screenshot shows a window titled "Main Switch" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The configuration commands entered are as follows:

```
Switch#
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Development
Switch(config-vlan)#
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Sales&Marketing
Switch(config-vlan)#
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name HumanResources
Switch(config-vlan)#
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name Finance
Switch(config-vlan)#
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name IT
Switch(config-vlan)#
Switch(config-vlan)#vlan 60
Switch(config-vlan)#name ConferencRoom
Switch(config-vlan)#
Switch(config-vlan)#vlan 70
Switch(config-vlan)#name ServerRoom
Switch(config-vlan)#
Switch(config-vlan)#vlan 99
Switch(config-vlan)#name Management
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#int range fa0/1,fa1/1,fa2/1,fa3/1,fa4/1,fa5/1,fa6/1,fa7/1,fa8/1,fa9/1
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99
Switch(config-if-range)#
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
Switch(config)#
Switch(config)#
```

At the bottom right of the CLI window, there are "Copy" and "Paste" buttons.

Figure 3core-switch vlan-config

This configuration is for the Main Switch (Core Switch), which connects all department switches and facilitates VLAN communication. VLANs 10-70 are created for different departments, with VLAN 99 designated for management. The trunk ports (Fa0/1 to Fa9/1) are configured to allow traffic from multiple VLANs to pass between the core switch, department switches, and the router. This setup enables inter-VLAN routing via the router-on-a-stick configuration while ensuring traffic remains isolated per VLAN.



## Router-on-a-Stick Configuration (Subinterfaces for VLAN Routing)

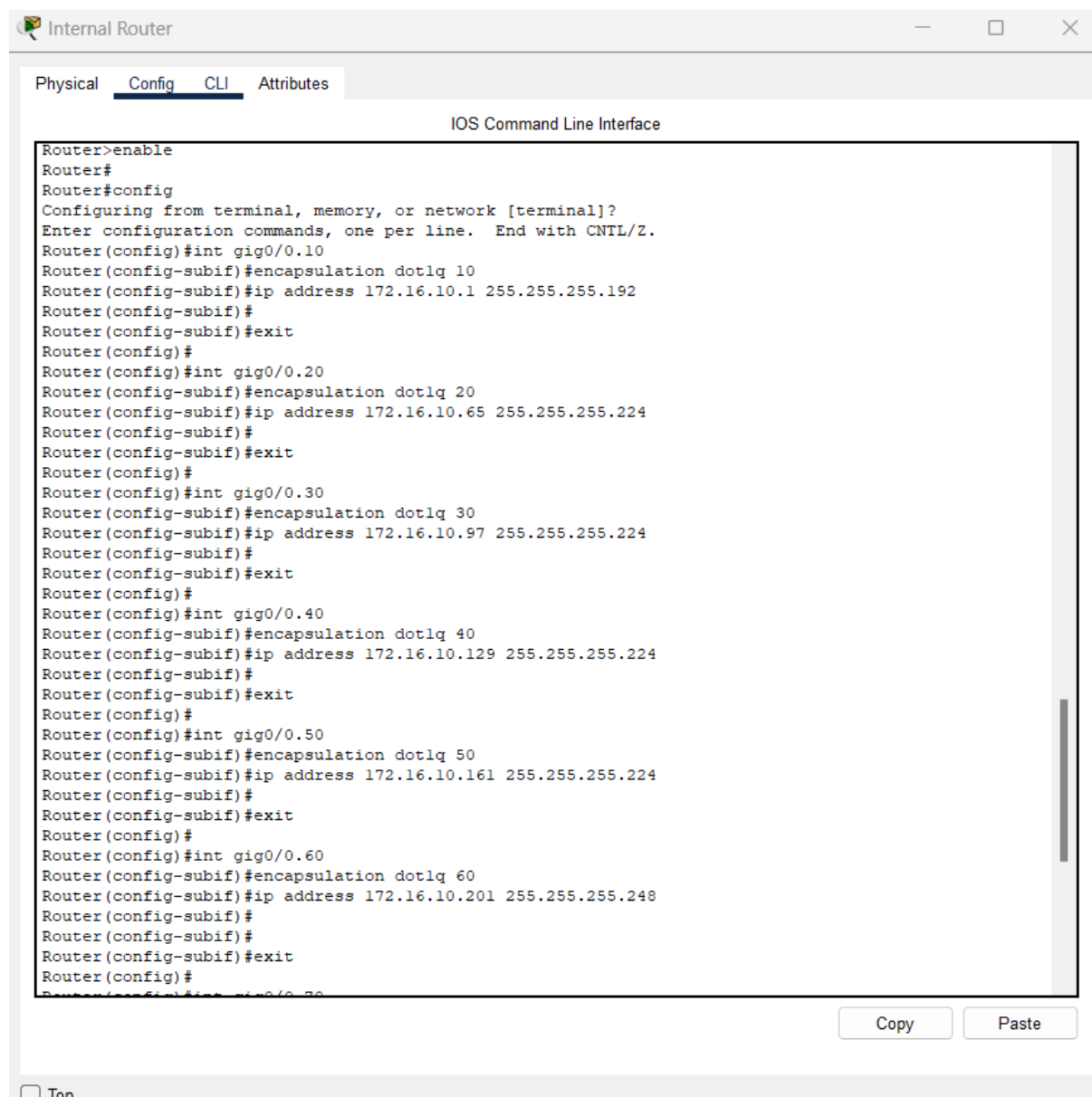


Figure 4 router vlan-config

```
Router(config)#int gig0/0.70
Router(config-subif)#encapsulation dot1q 70
Router(config-subif)#ip address 172.16.10.193 255.255.255.248
Router(config-subif)#
Router(config-subif)#exit
Router(config)#
Router(config)#
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#do wr
Building configuration...
[OK]
Router(config)#ex
```

Figure 5 router vlan-config pt2

This configuration is for the Internal Router, implementing a router-on-a-stick setup for inter-VLAN communication. Subinterfaces (gig0/0.x) are created for each VLAN, tagged with 802.1Q encapsulation. Each VLAN has a unique IP address (default gateway) assigned, allowing devices in that VLAN to route traffic through the router. This setup enables communication between VLANs while maintaining isolation. The subnet masks match each department's required host count.

## 2.5 DHCP Configuration

The DHCP server, present in the server room, was configured with a static IP address (172.16.10.194/29), a default gateway (172.16.10.193), and a DNS server (8.8.8.8) to ensure network stability.

Separate DHCP pools were created for each department, specifying the default gateway, subnet mask, and start IP range for each VLAN. For example, the Development VLAN uses 172.16.10.1 as its gateway and assigns IPs from 172.16.10.2 to 172.16.10.62.

After configuring all pools, the DHCP service was enabled, allowing dynamic IP allocation.

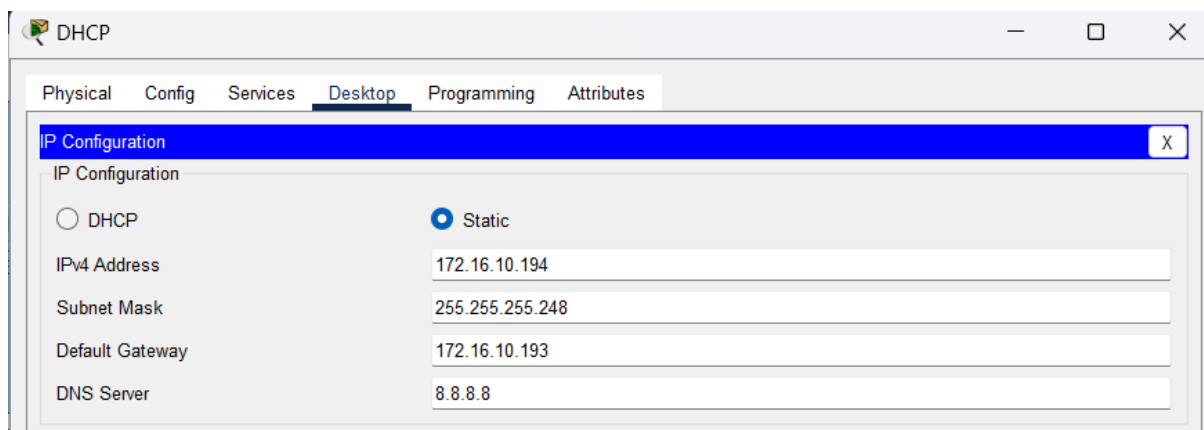


Figure 6Dhcp server ip

Physical

Config

Services

Desktop

Programming

Attributes

Services

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

Interface

FastEthernet0

Service

On

Off

Pool Name

Development

Default Gateway

172.16.10.1

DNS Server

8.8.8.8

Start IP Address :

172

16

10

2

Subnet Mask:

255

255

255

192

Maximum Number of Users :

50

TFTP Server:

0.0.0.0

WLC Address:

0.0.0.0

Add

Save

Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
ConferenceRoom	172.16.10.201	8.8.8.8	172.16.10.202	255.255.255.248	6	0.0.0.0	0.0.0.0
IT	172.16.10.161	8.8.8.8	172.16.10.162	255.255.255.224	20	0.0.0.0	0.0.0.0
Finance	172.16.10.129	8.8.8.8	172.16.10.130	255.255.255.224	25	0.0.0.0	0.0.0.0
HumanResources	172.16.10.97	8.8.8.8	172.16.10.98	255.255.255.224	25	0.0.0.0	0.0.0.0
Sales&Marketing	172.16.10.65	8.8.8.8	172.16.10.66	255.255.255.224	30	0.0.0.0	0.0.0.0
Development	172.16.10.1	8.8.8.8	172.16.10.2	255.255.255.192	50	0.0.0.0	0.0.0.0

Figure 7dhcp pools

To configure DHCP relay (IP helper-address) on your router, you need to add the IP helper address (which points to your DHCP server at 172.16.10.194) on each VLAN subinterface. This ensures that DHCP requests from clients are forwarded to the DHCP server.

11

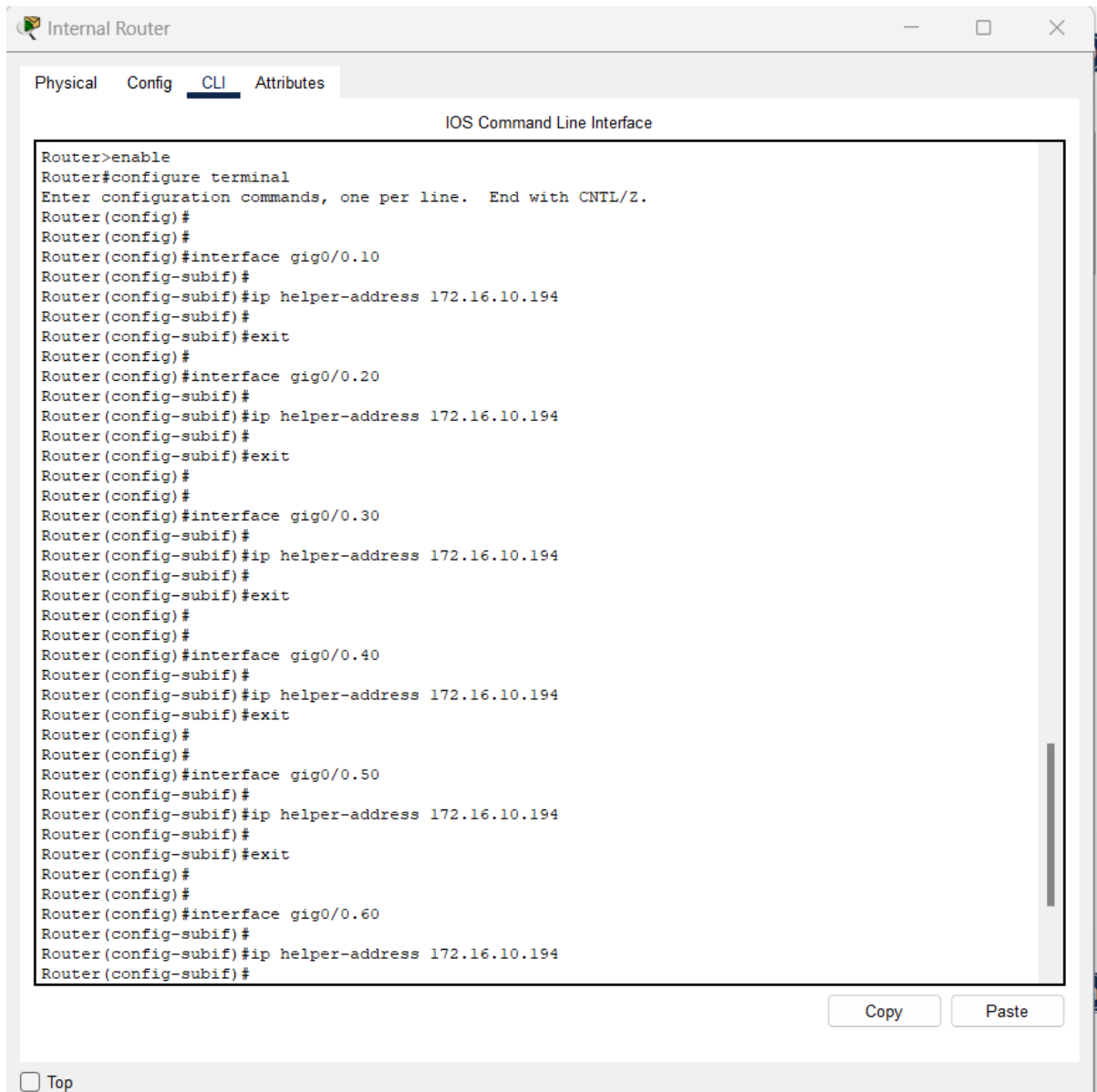


Figure 8 helper-address config

## DHCP Verification

DHCP is functioning correctly for a PC in VLAN 10 (Development Department). The PC successfully received an IP address (172.16.10.5) from the DHCP server, along with the correct subnet mask (255.255.255.192), default gateway (172.16.10.1), and DNS server (8.8.8.8).

This proves that DHCP relay (IP helper-address) is correctly forwarding requests, and the DHCP server is assigning IPs from the correct VLAN 10 pool. The successful DHCP request confirms that VLAN segmentation, trunking, and inter-VLAN routing are working properly

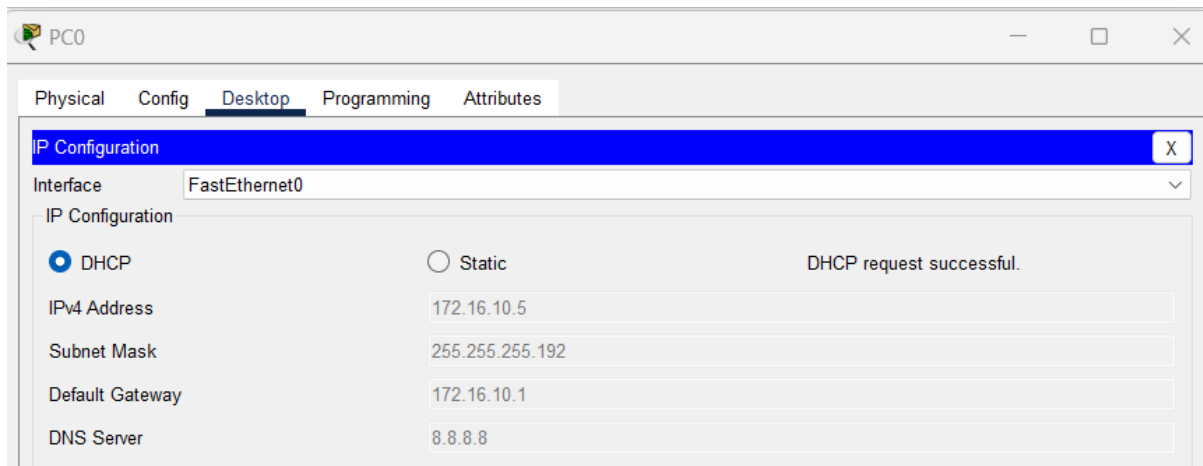


Figure 9dhcp assignment

### DHCP Justification

DHCP is essential for this network because it automates IP address allocation, reducing manual configuration errors. With multiple VLANs, DHCP ensures each device receives the correct IP, subnet mask, gateway, and DNS settings. It simplifies network management, enhances scalability

## 2.6 Routing Configuration

OSPF is not needed at this stage as only one router is in use

## 2.7 Wireless Network Configuration

After adding a wireless access point connecting to your main department switch, configure Port 1 on the access point by setting the SSID to the department name, selecting WPA2-PSK for security, and assigning a unique passkey.

Next, from a wireless device, I accessed the PC's wireless services, scanned for available networks, and connected to the Development department's access point using the passkey Dev12345@#.

This process was repeated for each department using their respective SSIDs and passwords:

SALES → Sales421@!

HR → HR3214\$@#

FINANCE → FIN4231@!

IT → IT4231%\$#@

Conference Room → CR3125@!#

Since this network consists of multiple VLANs with separate SSIDs, using WPA2-PSK with unique passkeys prevents unauthorized cross-department access while allowing easy authentication for employees.

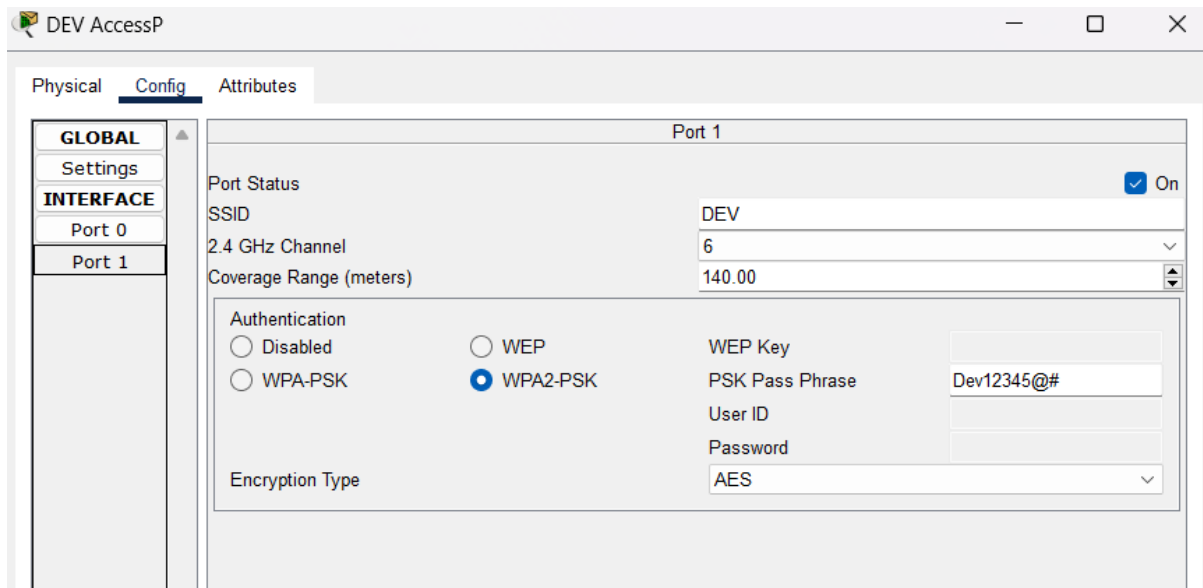


Figure 10 wireless setup

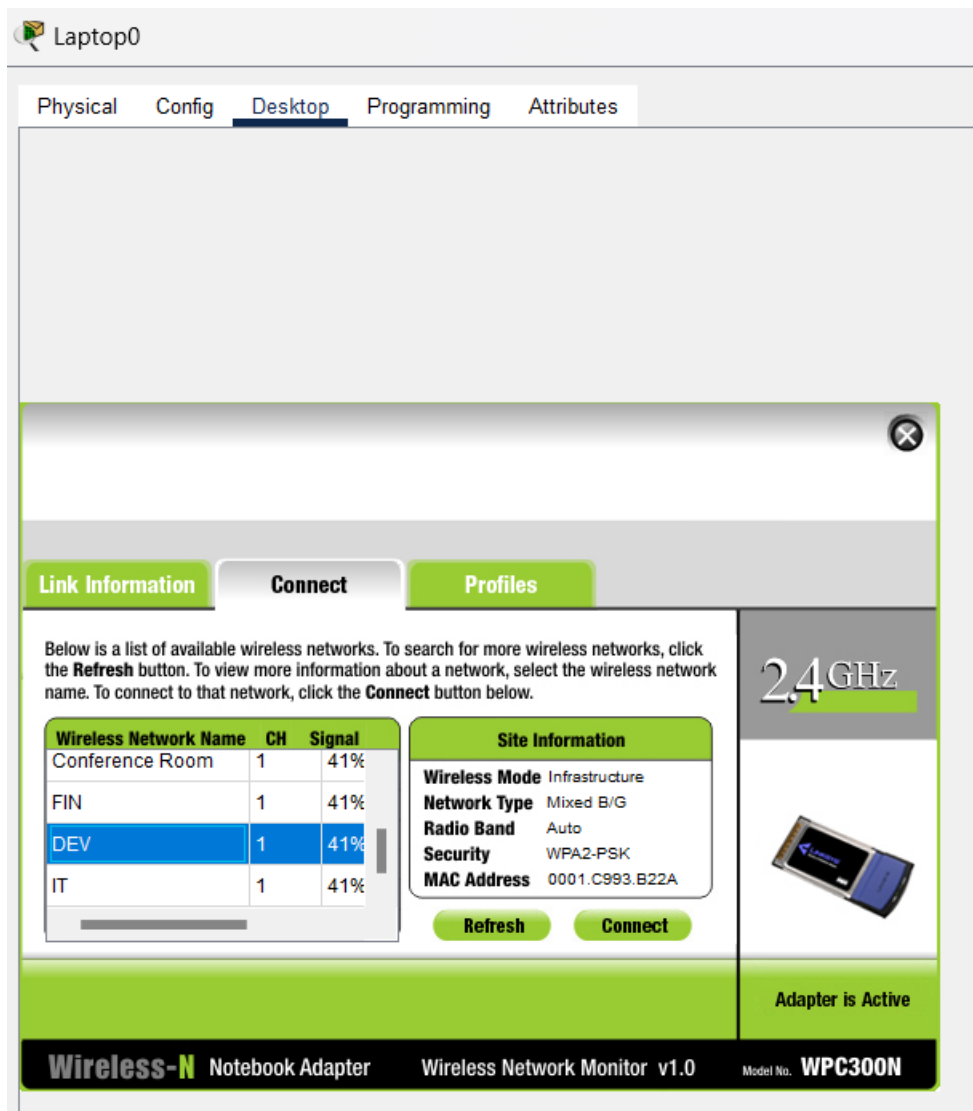


Figure 11 wireless connection pt1

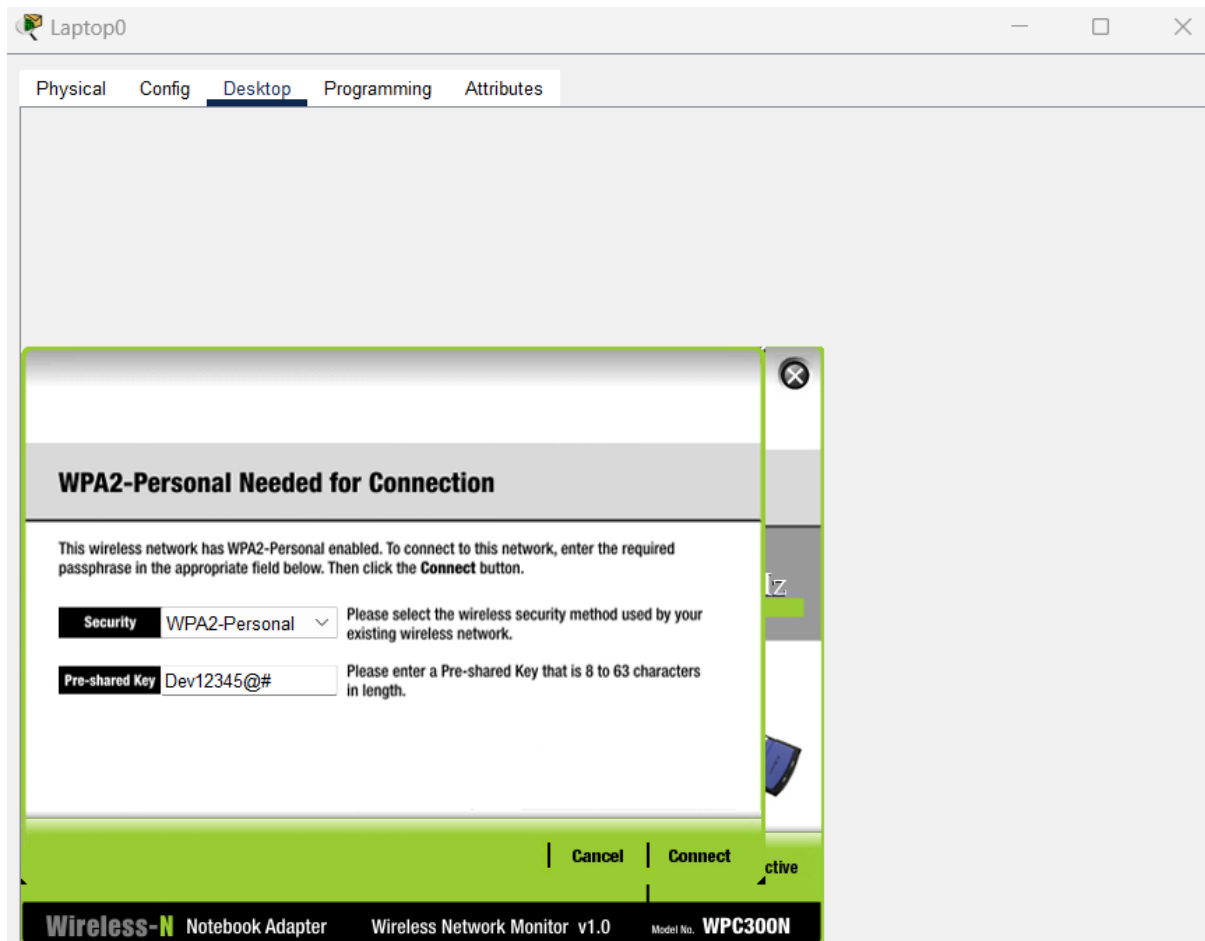


Figure 12 wireless connection pt2

## 2.8 Verification

Email server, web server functioning are used to show verification

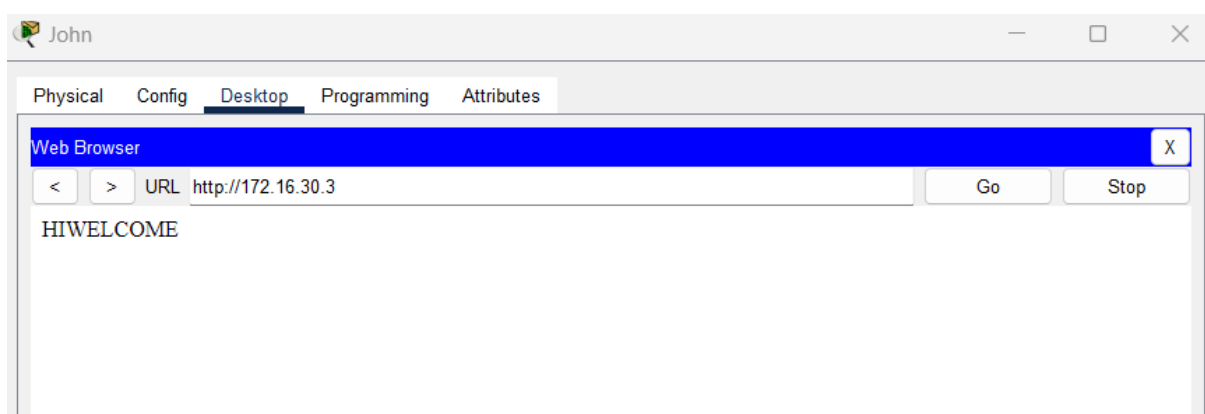


Figure 13 web server access

The PC in the Development subnet (VLAN 10) successfully accessed the web server in the server room (VLAN 70) using its IP address (172.16.30.3). This confirms that inter-VLAN routing

is working, allowing communication between different VLANs. The router-on-a-stick configuration is correctly handling traffic, and trunk ports on Layer 2 switches are properly forwarding packets. The web server is operational, responding to HTTP requests.

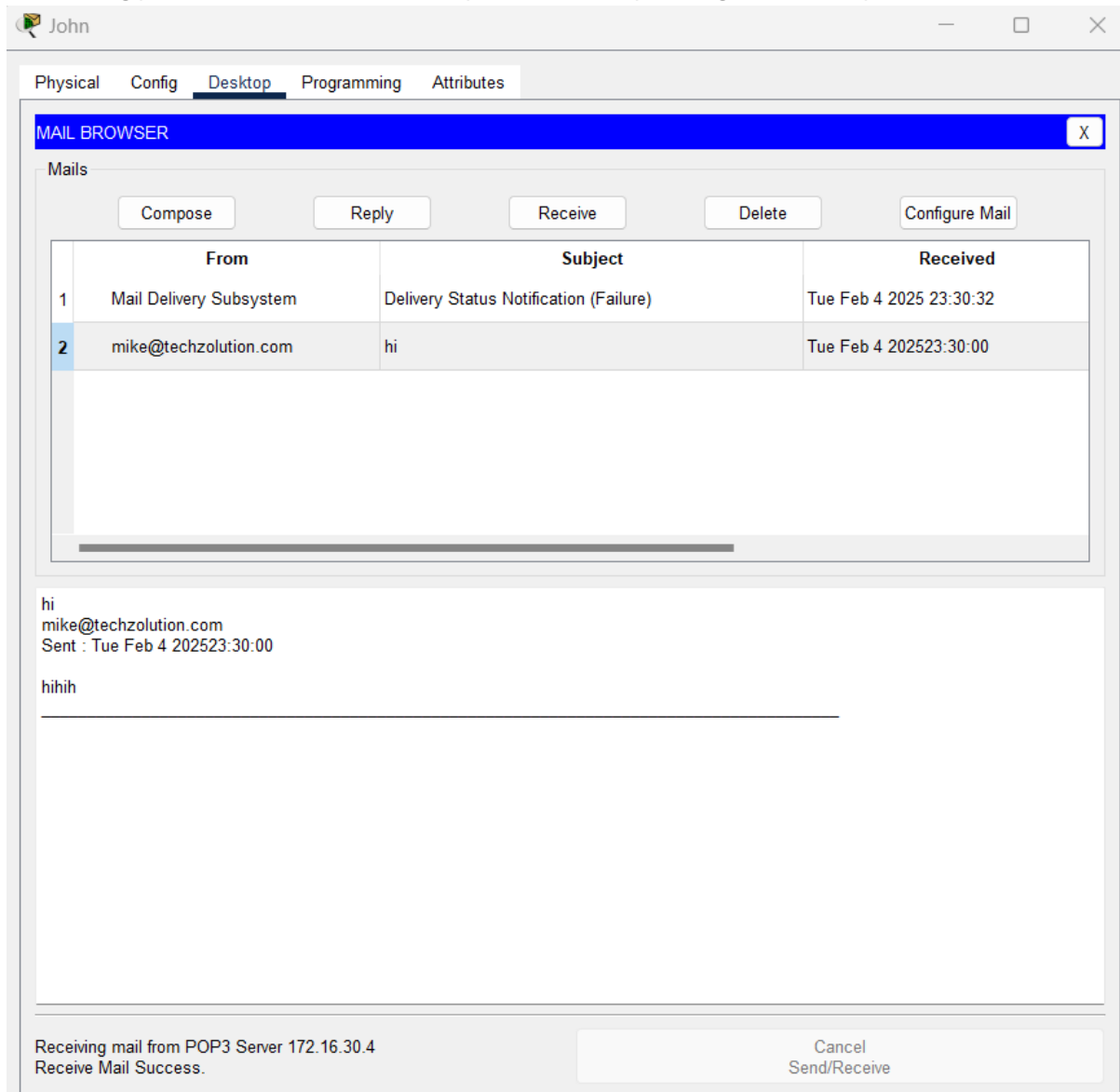


Figure 14 email server verification

The email client on John's PC (Development VLAN 10) shows a successfully received email from Mike (Sales VLAN 20) via techzolution.com, proving that inter-VLAN communication is working for email services. The POP3 server (172.16.30.4) in the server room (VLAN 70) successfully delivered the message, confirming proper SMTP and POP3 functionality. Additionally, the presence of a Mail Delivery Failure Notification suggests that outbound emails are being processed, though some may fail due to incorrect addresses or server restrictions. This demonstrates that employees from different departments, including Sales and Marketing, can communicate via email across VLANs.



### 3. Task 2: Security and Zones of Trust

#### 3.1 Security Measures on Network Devices

##### List of Device Passwords

Device	Device Password	Enable Secret Password
Internal Router	RouterPass123	RouterEnable123
Development Switch	DevPass123	RouterEnable123
Sales & Marketing Switch	SalesPass123	SalesEnable123
Human Resources Switch	HRPass123	HREnable123
Finance Switch	FinancePass123	FinanceEnable123
IT Switch	ITPass123	ITEnable123
Conference Room Switch	ConfPass123	ConfEnable123
Server Room Switch	ServerPass123	ServerEnable123

##### Commands to Configure Devices:

configure terminal

line console 0

password RouterPass123

login

exit

line vty 0 4

password RouterEnable123

login

exit

enable secret RouterEnable123

service password-encryption

exit

*(replace the passwords as per the table)*

Note:- AAA username and password for Internal Router

username **admin**

secret **StrongPassword123**

## 3.2 Zones of Trust

The network is divided into three security zones based on trust levels:

1. Internal Zone – Trusted corporate network (LAN).
2. DMZ (Demilitarized Zone) – Semi-trusted zone hosting public-facing services.
3. External Zone – Untrusted external internet and external branch

These zones are implemented using Cisco Zone-Based Firewall (ZBF), as seen in the screenshots.

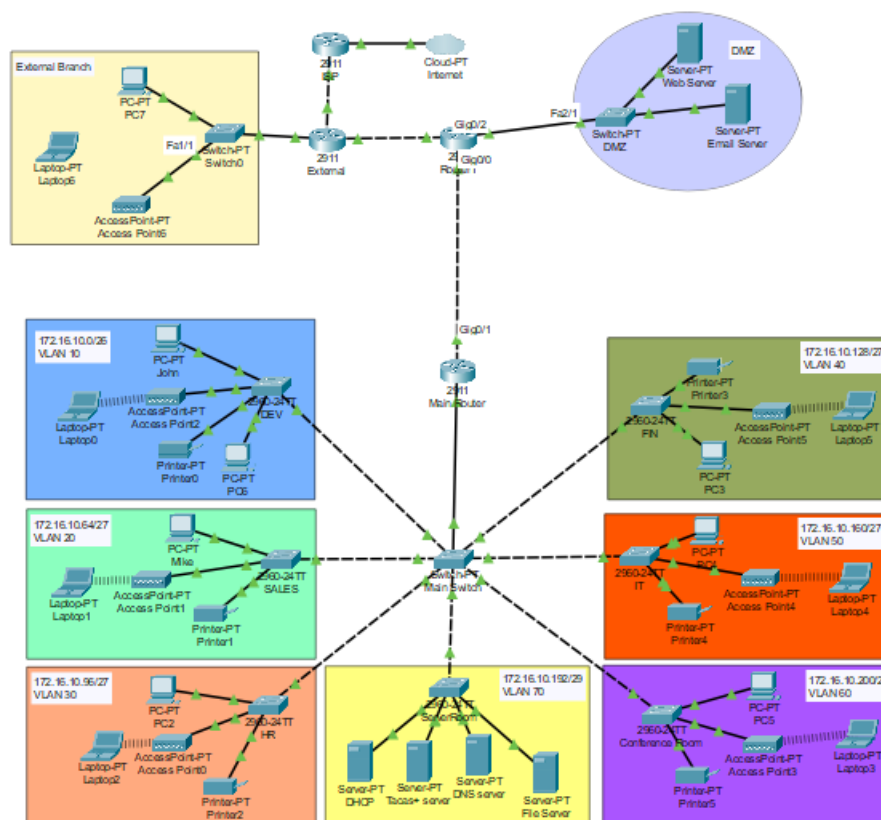


Figure 15 zones of trust

Dividing the network into zones of trust enhances security by limiting access based on risk levels. The Internal zone contains trusted corporate devices, including user workstations and departmental VLANs. This zone has restricted access to the external network, DMZ preventing direct exposure to cyber threats.

The DMZ (Demilitarized Zone) hosts public-facing servers (Web, and Email), allowing controlled external access while isolating these services from the internal network. This reduces the risk of direct attacks on sensitive internal systems. If a DMZ server is compromised, the attacker cannot directly access internal resources, minimizing damage.

The External zone represents the untrusted internet, which is highly vulnerable to attacks. Only essential traffic is permitted into the DMZ using Access Control Lists (ACLs) and Zone-Based Firewall (ZBF) policies. This prevents unauthorized access while ensuring necessary services remain available.

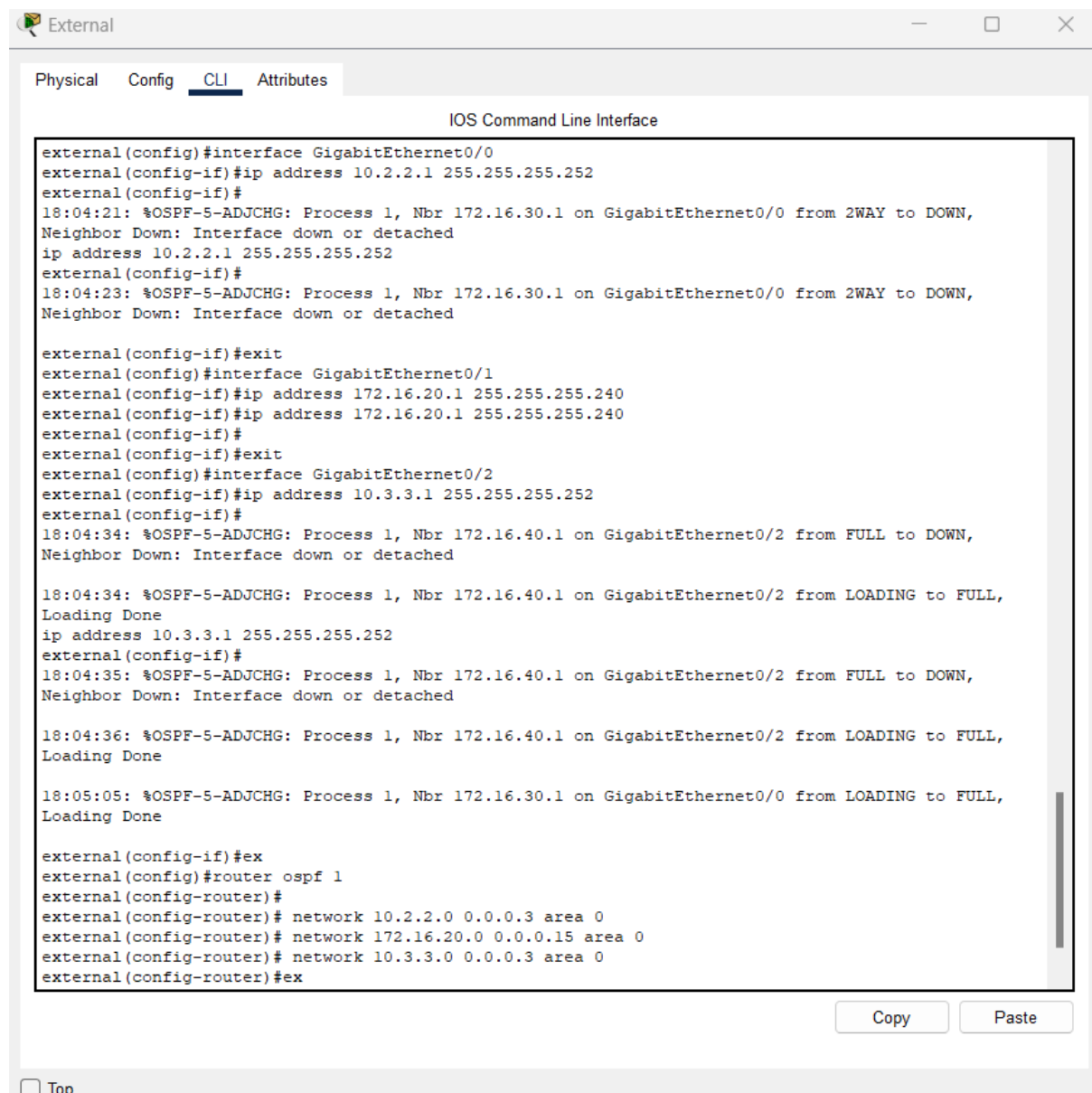
By implementing stateful inspection, only valid, established connections are allowed between zones. This prevents spoofing, unauthorized traffic, and lateral movement. The segmentation follows the principle of least privilege, allowing only necessary communications between zones.

This approach reduces the attack surface, improves monitoring, and enhances overall security, ensuring the network remains protected from cyber threats.

*(Note: the above can be used as a ZPF justification)*

## Configuration of the Zones

We need to configure all 4 routers in the network to have ospf to communicate with each other



```
external(config)#interface GigabitEthernet0/0
external(config-if)#ip address 10.2.2.1 255.255.255.252
external(config-if)#
18:04:21: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.30.1 on GigabitEthernet0/0 from 2WAY to DOWN,
Neighbor Down: Interface down or detached
ip address 10.2.2.1 255.255.255.252
external(config-if)#
18:04:23: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.30.1 on GigabitEthernet0/0 from 2WAY to DOWN,
Neighbor Down: Interface down or detached

external(config-if)#exit
external(config)#interface GigabitEthernet0/1
external(config-if)#ip address 172.16.20.1 255.255.255.240
external(config-if)#ip address 172.16.20.1 255.255.255.240
external(config-if)#
external(config-if)#exit
external(config)#interface GigabitEthernet0/2
external(config-if)#ip address 10.3.3.1 255.255.255.252
external(config-if)#
18:04:34: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.40.1 on GigabitEthernet0/2 from FULL to DOWN,
Neighbor Down: Interface down or detached

18:04:34: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.40.1 on GigabitEthernet0/2 from LOADING to FULL,
Loading Done
ip address 10.3.3.1 255.255.255.252
external(config-if)#
18:04:35: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.40.1 on GigabitEthernet0/2 from FULL to DOWN,
Neighbor Down: Interface down or detached

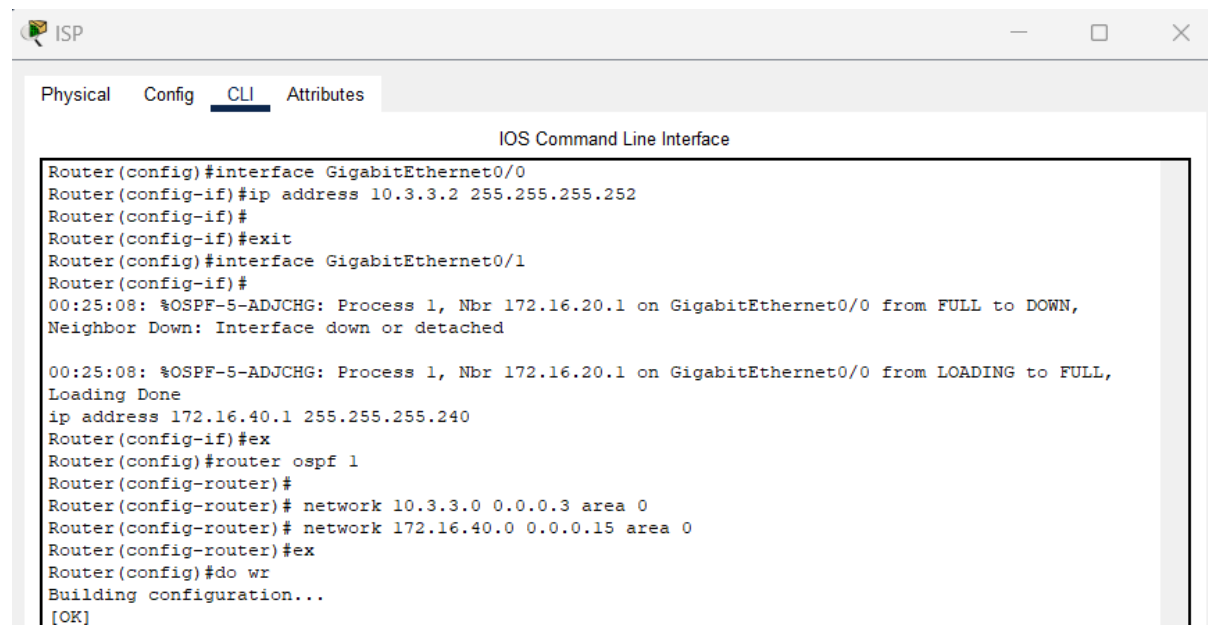
18:04:36: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.40.1 on GigabitEthernet0/2 from LOADING to FULL,
Loading Done

18:05:05: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.30.1 on GigabitEthernet0/0 from LOADING to FULL,
Loading Done

external(config-if)#ex
external(config)#router ospf 1
external(config-router)#
external(config-router)# network 10.2.2.0 0.0.0.3 area 0
external(config-router)# network 172.16.20.0 0.0.0.15 area 0
external(config-router)# network 10.3.3.0 0.0.0.3 area 0
external(config-router)#ex
```

Figure 16external router ospf config

The configuration shown is for an external router in an OSPF-enabled network. It sets IP addresses on GigabitEthernet0/0, 0/1, and 0/2, each with different subnets. The router is part of OSPF process 1, advertising networks 10.2.2.0/30, 172.16.20.0/28, and 10.3.3.0/30 in Area 0. This setup ensures dynamic routing between internal, external, and ISP networks, facilitating inter-network communication

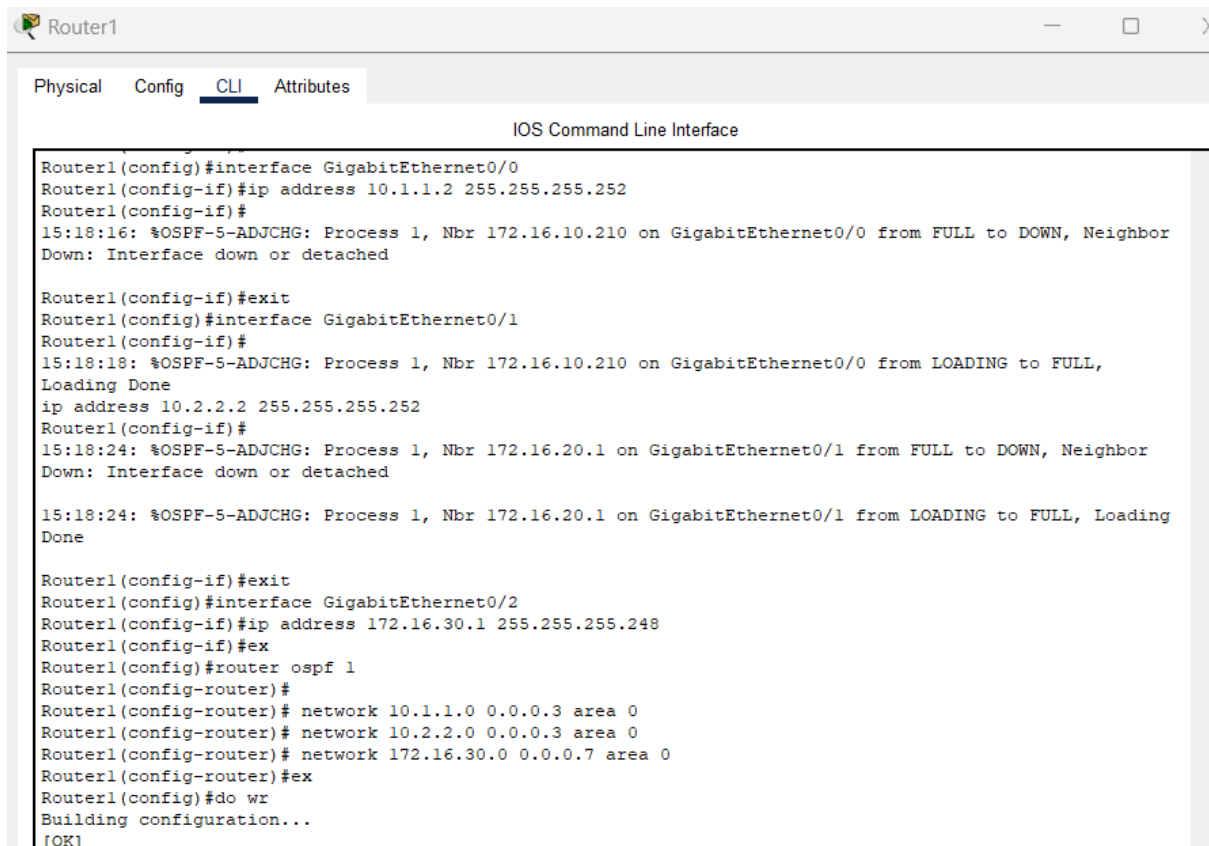


```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 10.3.3.2 255.255.255.252
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
00:25:08: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.20.1 on GigabitEthernet0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

00:25:08: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.20.1 on GigabitEthernet0/0 from LOADING to FULL,
Loading Done
ip address 172.16.40.1 255.255.255.240
Router(config-if)#ex
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)# network 10.3.3.0 0.0.0.3 area 0
Router(config-router)# network 172.16.40.0 0.0.0.15 area 0
Router(config-router)#ex
Router(config)#do wr
Building configuration...
[OK]
```

Figure 17isp router ospf config

The configuration is for an ISP router participating in OSPF process 1 to enable dynamic routing. It assigns 10.3.3.2/30 to GigabitEthernet0/0 and 172.16.40.1/24 to GigabitEthernet0/1. The router advertises 10.3.3.0/30 and 172.16.40.0/28 in OSPF Area 0, ensuring connectivity with the external router. This setup allows the ISP router to communicate with other routers in the network



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ip address 10.1.1.2 255.255.255.252
Router1(config-if)#
15:18:16: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.10.210 on GigabitEthernet0/0 from FULL to DOWN, Neighbor
Down: Interface down or detached

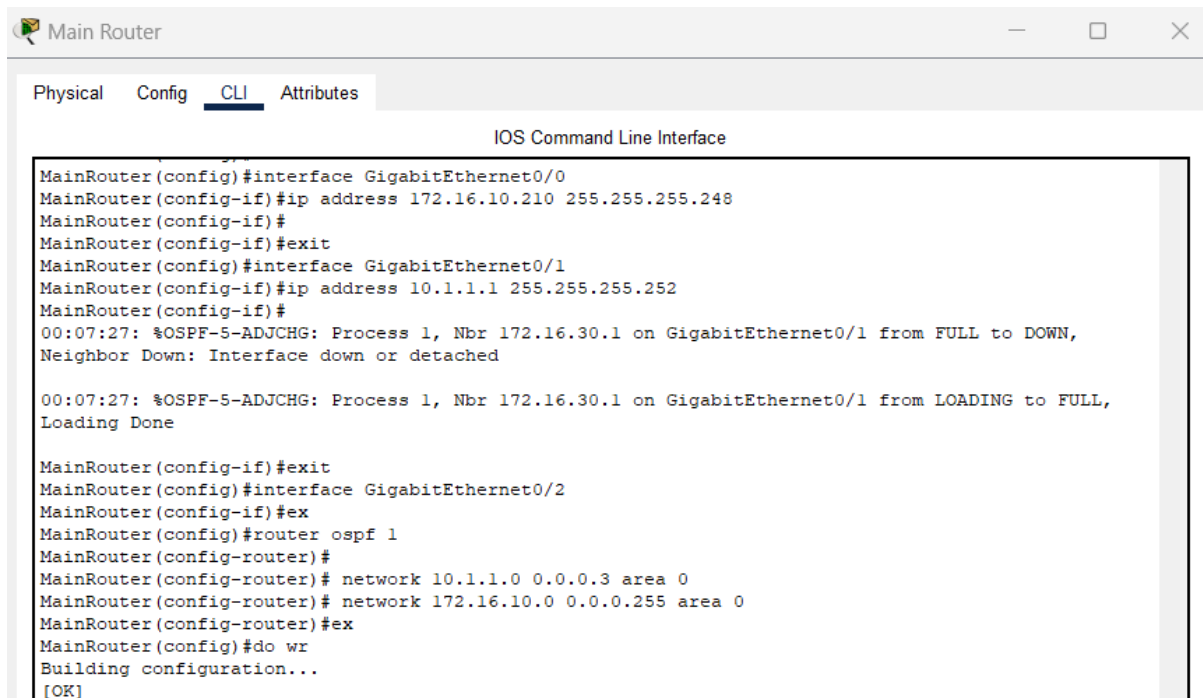
Router1(config-if)#exit
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)#
15:18:18: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.10.210 on GigabitEthernet0/0 from LOADING to FULL,
Loading Done
ip address 10.2.2.2 255.255.255.252
Router1(config-if)#
15:18:24: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.20.1 on GigabitEthernet0/1 from FULL to DOWN, Neighbor
Down: Interface down or detached

15:18:24: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.20.1 on GigabitEthernet0/1 from LOADING to FULL, Loading
Done

Router1(config-if)#exit
Router1(config)#interface GigabitEthernet0/2
Router1(config-if)#ip address 172.16.30.1 255.255.255.248
Router1(config-if)#ex
Router1(config)#router ospf 1
Router1(config-router)#
Router1(config-router)# network 10.1.1.0 0.0.0.3 area 0
Router1(config-router)# network 10.2.2.0 0.0.0.3 area 0
Router1(config-router)# network 172.16.30.0 0.0.0.7 area 0
Router1(config-router)#ex
Router1(config)#do wr
Building configuration...
[OK]
```

Figure 18 router1 ospf config

The configuration is for Router1, which participates in OSPF process 1 for dynamic routing. It assigns 10.1.1.2/30 to GigabitEthernet0/0, 10.2.2.2/30 to GigabitEthernet0/1, and 172.16.30.1/29 to GigabitEthernet0/2. The router advertises 10.1.1.0/30, 10.2.2.0/30, and 172.16.30.0/29 in OSPF Area 0. This setup ensures Router1 can dynamically share routes with other routers, facilitating communication

The screenshot shows a web-based interface for a 'Main Router'. At the top, there are tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs, the title 'IOS Command Line Interface' is displayed. The main area contains a text box with the following CLI commands and output:

```
MainRouter(config)#interface GigabitEthernet0/0
MainRouter(config-if)#ip address 172.16.10.210 255.255.255.248
MainRouter(config-if)#
MainRouter(config-if)#exit
MainRouter(config)#interface GigabitEthernet0/1
MainRouter(config-if)#ip address 10.1.1.1 255.255.255.252
MainRouter(config-if)#
00:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.30.1 on GigabitEthernet0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached

00:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.30.1 on GigabitEthernet0/1 from LOADING to FULL,
Loading Done

MainRouter(config-if)#exit
MainRouter(config)#interface GigabitEthernet0/2
MainRouter(config-if)#ex
MainRouter(config)#router ospf 1
MainRouter(config-router)#
MainRouter(config-router)# network 10.1.1.0 0.0.0.3 area 0
MainRouter(config-router)# network 172.16.10.0 0.0.0.255 area 0
MainRouter(config-router)#ex
MainRouter(config)#do wr
Building configuration...
[OK]
```

Figure 19 internal router ospf config

The Main Router is configured for OSPF process 1, enabling dynamic routing. It assigns 172.16.10.210/29 to GigabitEthernet0/0 and 10.1.1.1/30 to GigabitEthernet0/1. The router advertises 10.1.1.0/30 and 172.16.10.0/24 in OSPF Area 0. This setup allows the Main Router to exchange routing information dynamically, facilitating communication

### DMZ Config

After implementing the new security zones, the email and web servers were relocated to the DMZ and must be assigned static IP addresses within the 172.16.30.0/28 subnet. The email server will use 172.16.30.4, while the web server will be assigned 172.16.30.3. Additionally, the IP helper-address on the Main Router and all relevant subinterfaces must be updated to reflect these changes, ensuring proper forwarding of DHCP and other essential network services. This reconfiguration enhances security by isolating externally accessible services while maintaining seamless communication between the internal network and the DMZ.

## 3.3 Zone-Policy Firewall (ZPF) Configuration

first enable the security package for advanced firewall features on the router:

**license boot module c2900 technology-package securityk9**

Save the configuration:

**write memory**

Then, reload the router to apply changes:

**reload**

Once rebooted, you can proceed with ZBF configuration to secure traffic between Internal, DMZ, and External zones.

```
Router1#
Router1#
Router1#
Router1#
Router1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTRL/Z.
Router1(config)#zone security INTERNAL
Router1(config-sec-zone)#zone security DMZ
Router1(config-sec-zone)#zone security EXTERNAL
Router1(config-sec-zone)#exit
Router1(config)#
Router1(config)#
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)# description Internal Network
Router1(config-if)# zone-member security INTERNAL
Router1(config-if)# exit
Router1(config)#
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)# description DMZ Network
Router1(config-if)# zone-member security DMZ
Router1(config-if)# exit
Router1(config)#
Router1(config)#interface GigabitEthernet0/2
Router1(config-if)# description External Internet
Router1(config-if)# zone-member security EXTERNAL
Router1(config-if)# exit
Router1(config)#
Router1(config)#ip access-list extended INTERNAL-DMZ-TRAFFIC
Router1(config-ext-nacl)#
Router1(config-ext-nacl)#access-list 100 permit tcp any any eq 25
Router1(config)#access-list 100 permit tcp any any eq 587
Router1(config)#access-list 100 permit tcp any any eq 110
Router1(config)#access-list 100 permit tcp any any eq 80
Router1(config)#access-list 100 permit tcp any any eq 443
Router1(config)#access-list 100 permit udp any any eq 53
Router1(config)#access-list 100 permit tcp any any eq 53
Router1(config)#access-list 100 permit udp any any eq 123
Router1(config)#access-list 100 permit icmp any any echo
Router1(config)#access-list 100 permit icmp any any echo-reply
Router1(config)#
Router1(config)#
```

Figure 20zpf config pt1

The configuration on Router1 sets up Zone-Based Firewall (ZBF) by defining three security zones: INTERNAL, DMZ, and EXTERNAL. Each interface is assigned to a specific zone to control traffic flow.

An Access Control List (ACL) named INTERNAL-DMZ-TRAFFIC is created to permit essential services like SMTP (25, 587), POP3 (110), HTTP (80), HTTPS (443), DNS (53), and ICMP (ping/echo) between the Internal and DMZ zones.

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

Router1(config)#ip access-list extended DMZ-EXTERNAL-TRAFFIC
Router1(config-ext-nacl)#access-list 101 permit tcp any any eq 25
Router1(config)#access-list 101 permit tcp any any eq 587
Router1(config)#access-list 101 permit tcp any any eq 110
Router1(config)#access-list 101 permit tcp any any eq 80
Router1(config)#access-list 101 permit tcp any any eq 443
Router1(config)#access-list 101 permit udp any any eq 53
Router1(config)#access-list 101 permit tcp any any eq 53
Router1(config)#access-list 101 permit udp any any eq 123
Router1(config)#access-list 101 permit icmp any any echo
Router1(config)#access-list 101 permit icmp any any echo-reply
Router1(config)#access-list 101 permit tcp any any
Router1(config)#access-list 101 permit udp any any
Router1(config)#access-list 101 permit ICMP any any
Router1(config)#
Router1(config)#
Router1(config)#ex
Router1#
%SYS-5-CONFIG_I: Configured from console by console
config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#
Router1(config)#
Router1(config)#ip access-list extended INTERNAL-EXTERNAL-TRAFFIC
Router1(config-ext-nacl)#access-list 102 permit tcp any any eq 25
Router1(config)#access-list 102 permit tcp any any eq 587
Router1(config)#access-list 102 permit tcp any any eq 110
Router1(config)#access-list 102 permit tcp any any eq 80
Router1(config)#access-list 102 permit tcp any any eq 443
Router1(config)#access-list 102 permit udp any any eq 53
Router1(config)#access-list 102 permit tcp any any eq 53
Router1(config)#access-list 102 permit udp any any eq 123
Router1(config)#access-list 102 permit icmp any any echo
Router1(config)#access-list 102 permit icmp any any echo-reply
Router1(config)#access-list 102 permit tcp any any eq 20
Router1(config)#access-list 102 permit tcp any any eq 21
Router1(config)#access-list 102 permit tcp any any eq 445
Router1(config)#access-list 102 permit tcp any any eq 2049
Router1(config)#access-list 102 permit tcp any any
Router1(config)#access-list 102 permit udp any any
Router1(config)#access-list 102 permit ICMP any any
```

Copy Paste

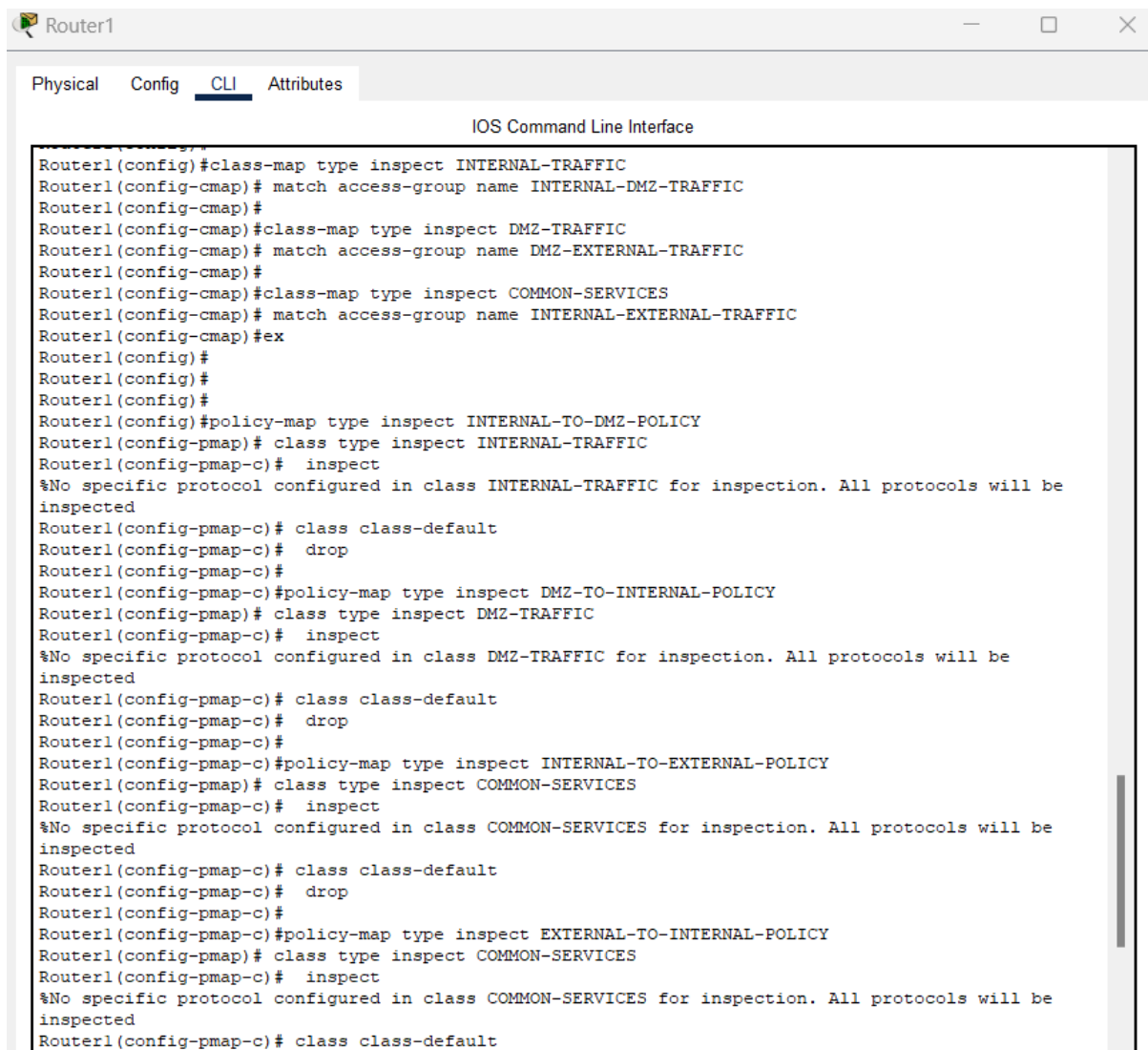
Figure 21zpf config pt2

The configuration on Router1 defines two additional Access Control Lists (ACLs) to regulate traffic between zones.

DMZ-EXTERNAL-TRAFFIC (ACL 101): Controls traffic from the DMZ to the External (Internet) zone, permitting services like SMTP (25, 587), POP3 (110), HTTP (80), HTTPS (443), DNS (53), and ICMP (ping/echo).

INTERNAL-EXTERNAL-TRAFFIC (ACL 102): Manages traffic from the Internal network to the External zone, allowing additional services like FTP (21), SFTP (22), and IMAP (143, 993).





```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

Router1(config)#class-map type inspect INTERNAL-TRAFFIC
Router1(config-cmap)# match access-group name INTERNAL-DMZ-TRAFFIC
Router1(config-cmap)#
Router1(config-cmap)#class-map type inspect DMZ-TRAFFIC
Router1(config-cmap)# match access-group name DMZ-EXTERNAL-TRAFFIC
Router1(config-cmap)#
Router1(config-cmap)#class-map type inspect COMMON-SERVICES
Router1(config-cmap)# match access-group name INTERNAL-EXTERNAL-TRAFFIC
Router1(config-cmap)#ex
Router1(config)#
Router1(config)#
Router1(config)#
Router1(config)#policy-map type inspect INTERNAL-TO-DMZ-POLICY
Router1(config-pmap)# class type inspect INTERNAL-TRAFFIC
Router1(config-pmap-c)# inspect
%No specific protocol configured in class INTERNAL-TRAFFIC for inspection. All protocols will be inspected
Router1(config-pmap-c)# class class-default
Router1(config-pmap-c)# drop
Router1(config-pmap-c)#
Router1(config-pmap-c)#policy-map type inspect DMZ-TO-INTERNAL-POLICY
Router1(config-pmap)# class type inspect DMZ-TRAFFIC
Router1(config-pmap-c)# inspect
%No specific protocol configured in class DMZ-TRAFFIC for inspection. All protocols will be inspected
Router1(config-pmap-c)# class class-default
Router1(config-pmap-c)# drop
Router1(config-pmap-c)#
Router1(config-pmap-c)#policy-map type inspect INTERNAL-TO-EXTERNAL-POLICY
Router1(config-pmap)# class type inspect COMMON-SERVICES
Router1(config-pmap-c)# inspect
%No specific protocol configured in class COMMON-SERVICES for inspection. All protocols will be inspected
Router1(config-pmap-c)# class class-default
Router1(config-pmap-c)# drop
Router1(config-pmap-c)#
Router1(config-pmap-c)#policy-map type inspect EXTERNAL-TO-INTERNAL-POLICY
Router1(config-pmap)# class type inspect COMMON-SERVICES
Router1(config-pmap-c)# inspect
%No specific protocol configured in class COMMON-SERVICES for inspection. All protocols will be inspected
Router1(config-pmap-c)# class class-default
```

Figure 22zpf config pt3

This configuration on Router1 defines class maps and policy maps for Zone-Based Firewall (ZBF) to control traffic flow between zones.

#### Class Maps:

- Match ACLs for INTERNAL-DMZ, DMZ-EXTERNAL, and INTERNAL-EXTERNAL traffic.
- The COMMON-SERVICES class inspects general traffic rules.

#### Policy Maps:

- INTERNAL-TO-DMZ-POLICY and DMZ-TO-INTERNAL-POLICY inspect traffic between internal resources and the DMZ.
- INTERNAL-TO-EXTERNAL and EXTERNAL-TO-INTERNAL control internet-bound traffic.
- Unmatched traffic is dropped by default.

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router1(config-pmap-c)#policy-map type inspect DMZ-TO-EXTERNAL-POLICY
Router1(config-pmap)# class type inspect DMZ-TRAFFIC
Router1(config-pmap-c)# inspect
%No specific protocol configured in class DMZ-TRAFFIC for inspection. All protocols will be inspected
Router1(config-pmap-c)# class class-default
Router1(config-pmap-c)# drop
Router1(config-pmap-c)#
Router1(config-pmap-c)#policy-map type inspect EXTERNAL-TO-DMZ-POLICY
Router1(config-pmap)# class type inspect DMZ-TRAFFIC
Router1(config-pmap-c)# inspect
%No specific protocol configured in class DMZ-TRAFFIC for inspection. All protocols will be inspected
Router1(config-pmap-c)# class class-default
Router1(config-pmap-c)# drop
Router1(config-pmap-c)#ex
Router1(config-pmap)#ex
Router1(config)#
Router1(config)#zone-pair security INTERNAL-TO-DMZ source INTERNAL destination DMZ
Router1(config-sec-zone-pair)# service-policy type inspect INTERNAL-TO-DMZ-POLICY
Router1(config-sec-zone-pair)#
Router1(config-sec-zone-pair)#zone-pair security DMZ-TO-INTERNAL source DMZ destination INTERNAL
Router1(config-sec-zone-pair)# service-policy type inspect DMZ-TO-INTERNAL-POLICY
Router1(config-sec-zone-pair)#
Router1(config-sec-zone-pair)#zone-pair security INTERNAL-TO-EXTERNAL source INTERNAL destination EXTERNAL
Router1(config-sec-zone-pair)# service-policy type inspect INTERNAL-TO-EXTERNAL-POLICY
Router1(config-sec-zone-pair)#
Router1(config-sec-zone-pair)#zone-pair security EXTERNAL-TO-INTERNAL source EXTERNAL destination INTERNAL
Router1(config-sec-zone-pair)# service-policy type inspect EXTERNAL-TO-INTERNAL-POLICY
Router1(config-sec-zone-pair)#
Router1(config-sec-zone-pair)#zone-pair security DMZ-TO-EXTERNAL source DMZ destination EXTERNAL
Router1(config-sec-zone-pair)# service-policy type inspect DMZ-TO-EXTERNAL-POLICY
Router1(config-sec-zone-pair)#
Router1(config-sec-zone-pair)#zone-pair security EXTERNAL-TO-DMZ source EXTERNAL destination DMZ
Router1(config-sec-zone-pair)# service-policy type inspect EXTERNAL-TO-DMZ-POLICY
Router1(config-sec-zone-pair)#ex
Router1(config)#do wr
Building configuration...
[OK]
Router1(config)#
```

Copy Paste

Figure 23zpf config pt5

This configuration on Router1 applies Zone-Based Firewall (ZBF) policies to enforce traffic control between security zones.

#### Policy Maps:

- Define inspection rules for traffic between zones, ensuring stateful inspection.
- Unmatched traffic is dropped by default.

#### Zone-Pair Security Assignments:

- Traffic from INTERNAL to DMZ follows the INTERNAL-TO-DMZ-POLICY.
- DMZ to INTERNAL uses DMZ-TO-INTERNAL-POLICY.
- INTERNAL to EXTERNAL and EXTERNAL to INTERNAL traffic is inspected separately.
- DMZ to EXTERNAL follows its own policy for public-facing services.

## ZPF Verification

The Zone-Based Firewall (ZPF) is functioning correctly, ensuring secure access to network services. The email service (POP3) and web service (HTTP) are accessible from both internal and external branches, confirming that traffic filtering and inspection policies are correctly applied. Additionally, FTP access is available between the internal and external zones, verifying that authorized traffic is permitted while unauthorized traffic is blocked. The configured security zones and policies effectively control communication between the Internal, DMZ, and External zones

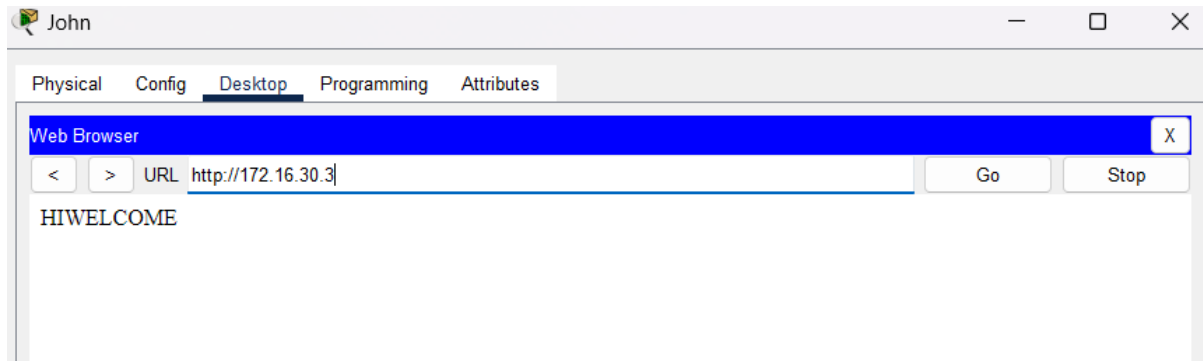


Figure 24web server verification

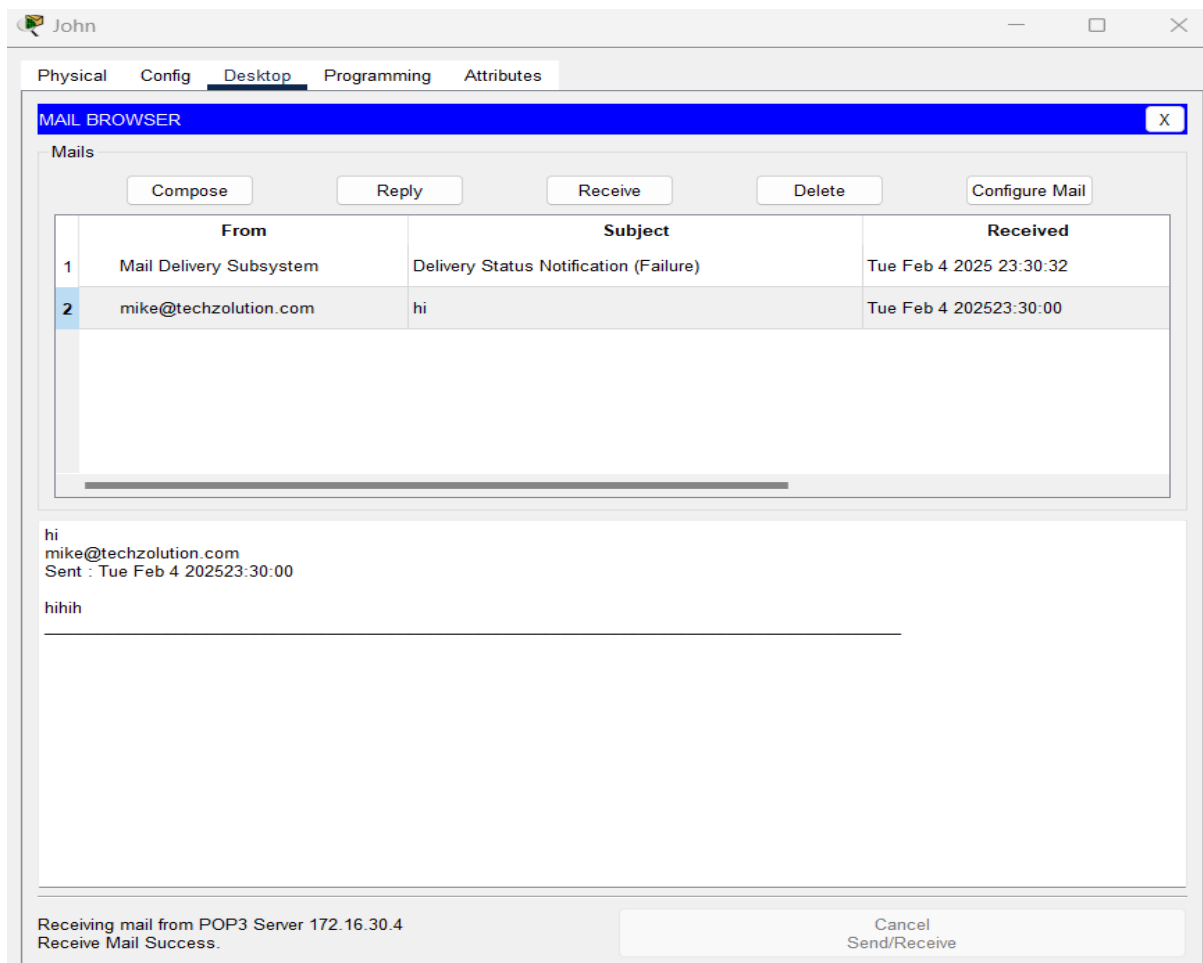


Figure 25email server verification

### 3.4 Access Control Lists (ACLs)

To configure ACLs on the internal network, they must be applied where inter-VLAN routing is performed, which in this case is on the MainRouter. Since VLANs are segmented networks, ACLs need to be assigned to the router's subinterfaces, where routing between VLANs occurs.

Each VLAN requires its own ACL to control traffic flow based on department-specific security policies. For example, if HR should not initiate communication with Development, an ACL on the Development VLAN's subinterface can block inbound traffic from HR while still allowing Development to communicate with HR. Similarly, Finance can be restricted from accessing sensitive HR data while retaining access to financial servers.

In the provided configuration, an ACL was applied to the Development VLAN's subinterface (Gig0/0.10), restricting ICMP (ping) requests from HR while allowing replies. This ensures HR cannot ping Development, but Development can still reach HR and receive responses. Similarly each of the sub interfaces need access-lists to permit and deny necessary traffic

```
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)# no ip access-group DEV-ACL in
Router(config-subif)# exit
Router(config)#no ip access-list extended DEV-ACL
Router(config)#ip access-list extended DEV-ACL
Router(config-ext-nacl)# deny icmp 172.16.10.96 0.0.0.31 172.16.10.0 0.0.0.63 echo
Router(config-ext-nacl)# permit icmp 172.16.10.96 0.0.0.31 172.16.10.0 0.0.0.63 echo-reply
Router(config-ext-nacl)#deny ip 172.16.10.0 0.0.0.63 172.16.10.96 0.0.0.31
Router(config-ext-nacl)# deny ip 172.16.10.0 0.0.0.63 172.16.10.128 0.0.0.31
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)#ex
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)# ip access-group DEV-ACL in
Router(config-subif)#ex
```

Figure 26 Internal ACL config

## 4. Task 3: Advanced Security Configuration

### 4.1 Site-to-Site VPN Configuration

To enable advanced security features like IPsec VPN, firewall, and encryption, activate the securityk9 license on the router. Enter global configuration mode:

**config terminal**

**license boot module c2900 technology-package securityk9**

Accept the license agreement when prompted by entering "yes". Then, save the configuration:

**do wr**

Finally, reload the router to apply changes:

**reload**

Once the router restarts, security features will be enabled, allowing VPN this is config has to be done both on the external and internal router which the vpn tunnel will be done from

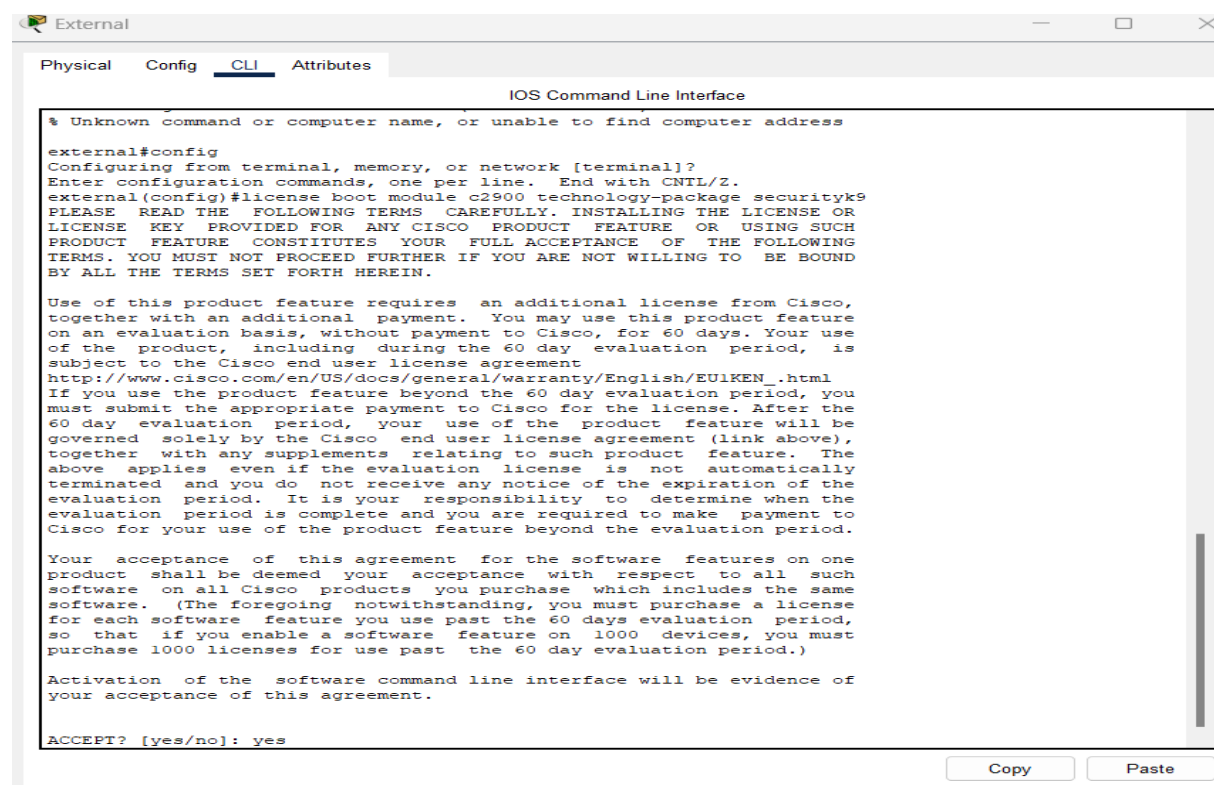


Figure 27vpn config pt1

```

external>en
external#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
external(config)#access-list 110 permit ip 172.16.20.0 0.0.0.15 172.16.10.0 0.0.0.255
external(config)#crypto isakmp policy 10
external(config-isakmp)#
00:00:55: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.40.1 on GigabitEthernet0/2 from LOADING to FULL,
Loading Done

00:00:55: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.30.1 on GigabitEthernet0/0 from LOADING to FULL,
Loading Done
encryption aes 256
external(config-isakmp)#authentication pre-share
external(config-isakmp)#group 5
external(config-isakmp)#exit
external(config)#crypto isakmp key vpnpa55 address 10.1.1.1
external(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
external(config)# crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
external(config-crypto-map)#description VPN connection to MainRouter
external(config-crypto-map)#set peer 10.1.1.1
external(config-crypto-map)#set transform-set VPN-SET
external(config-crypto-map)#match address 110
external(config-crypto-map)#exit
external(config)#interface gig0/0
external(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
external(config-if)#

```

Figure 28vpn config external-router

This configuration sets up a secure VPN connection between the External Router and the MainRouter using IPsec.

First, an access control list (ACL 110) is created to specify which network traffic should be encrypted. Then, an ISAKMP policy is configured to define how the two routers will securely exchange encryption keys, using AES 256 encryption and pre-shared key authentication.

Next, an IPsec transform set is created to ensure data is encrypted and verified for integrity. A crypto map is then set up to link the VPN settings to the correct remote router. Finally, this crypto map is applied to GigabitEthernet0/0, activating the VPN connection.

```

Username: admin
Password:
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 110 permit ip 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.15
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
00:00:55: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.30.1 on GigabitEthernet0/1 from LOADING to FULL,
Loading Done

Router(config)#crypto isakmp key vpnpa55 address 10.2.2.1
Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Router(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#description VPN connection to ExternalR
Router(config-crypto-map)#set peer 10.2.2.1
Router(config-crypto-map)#set transform-set VPN-SET
Router(config-crypto-map)#match address 110
Router(config-crypto-map)#exit
Router(config)#interface gig0/1
Router(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#

```

Figure 29vpn config internal-router

This configuration sets up an IPsec VPN on a router. The access-list 110 defines interesting traffic between 172.16.10.0/24 and 172.16.20.0/28, which will trigger the VPN. The IKE Phase 1 ISAKMP policy (policy 10) is configured with AES-256 encryption, pre-shared authentication, and DH Group 5 for key exchange. A shared key (vpnpa55) is set for peer 10.2.2.1. In IKE Phase 2, a transform set (VPN-SET) is created using ESP-AES and ESP-SHA-HMAC. A crypto map (VPN-MAP) binds these settings and is applied to interface GigabitEthernet0/1, enabling ISAKMP (ISAKMP is ON).

```

Router1(config)#
Router1(config)# ip access-list extended VPN-TRAFFIC-ACL
Router1(config-ext-nacl)# permit esp any any
Router1(config-ext-nacl)# permit udp any any eq isakmp
Router1(config-ext-nacl)# permit udp any any eq 4500
Router1(config-ext-nacl)# exit
Router1(config)#
Router1(config)#
Router1(config)#
Router1(config)# class-map type inspect VPN-TRAFFIC
Router1(config-cmap)# match access-group name VPN-TRAFFIC-ACL
Router1(config-cmap)# exit
Router1(config)#
Router1(config)# policy-map type inspect ALLOW-VPN-POLICY
Router1(config-pmap)# class type inspect VPN-TRAFFIC
Router1(config-pmap-c)# pass
Router1(config-pmap-c)# exit
Router1(config-pmap)# class class-default
Router1(config-pmap-c)# drop
Router1(config-pmap-c)# exit
Router1(config-pmap)#
Router1(config-pmap)# zone-pair security INTERNAL-TO-EXTERNAL source INTERNAL destination EXTERNAL
Router1(config-sec-zone-pair)# service-policy type inspect ALLOW-VPN-POLICY
Router1(config-sec-zone-pair)# exit
Router1(config)#
Router1(config)# zone-pair security EXTERNAL-TO-INTERNAL source EXTERNAL destination INTERNAL
Router1(config-sec-zone-pair)# service-policy type inspect ALLOW-VPN-POLICY
Router1(config-sec-zone-pair)# exit
Router1(config)#

```

Figure 30add vpn to zpf security

This Zone Pair configuration on Router1 allows VPN traffic while maintaining security. An ACL (VPN-TRAFFIC-ACL) permits ESP, ISAKMP (UDP 500), and NAT-T (UDP 4500). A class map (VPN-TRAFFIC) matches this ACL, and a policy map (ALLOW-VPN-POLICY) ensures VPN traffic is



passed while blocking unclassified traffic. Zone pairs (INTERNAL-TO-EXTERNAL and EXTERNAL-TO-INTERNAL) apply this policy, allowing bidirectional VPN traffic. This prevents Router1's ZBF from blocking VPN communication, ensuring encrypted traffic between Internal (Main Router) and External (External Router) networks while maintaining firewall security.

```
external#show crypto ipsec sa

interface: GigabitEthernet0/0
  Crypto map tag: VPN-MAP, local addr 10.2.2.1

protected vrf: (none)
local  ident (addr/mask/prot/port): (172.16.20.0/255.255.255.240/0/0)
remote  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
current_peer 10.1.1.1 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 0
#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.2.2.1, remote crypto endpt.:10.1.1.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0xE6FD4C1A(3875359770)

inbound esp sas:
  spi: 0xB7E24BAE(3085061038)

--More--
```

Figure 31vpn verification

This IPsec Security Association (SA) status shows an active VPN tunnel between 10.2.2.1 (local) and 10.1.1.1 (remote). Packets are being encrypted (10) and encapsulated,

## Justification of VPN

A site-to-site VPN was needed for this network to ensure secure, encrypted communication between geographically separate locations. Since this network connects an internal LAN (172.16.10.0/24) with an external network (172.16.20.0/28) via Router1, traffic traveling between them would otherwise be exposed to potential interception, eavesdropping, or unauthorized access.

A VPN eliminates these risks by creating an encrypted tunnel over an untrusted medium (such as the internet or a shared network), ensuring data integrity, confidentiality, and authenticity. Without a VPN, sensitive business data, authentication credentials, and confidential transactions could be at risk of being intercepted by attackers.

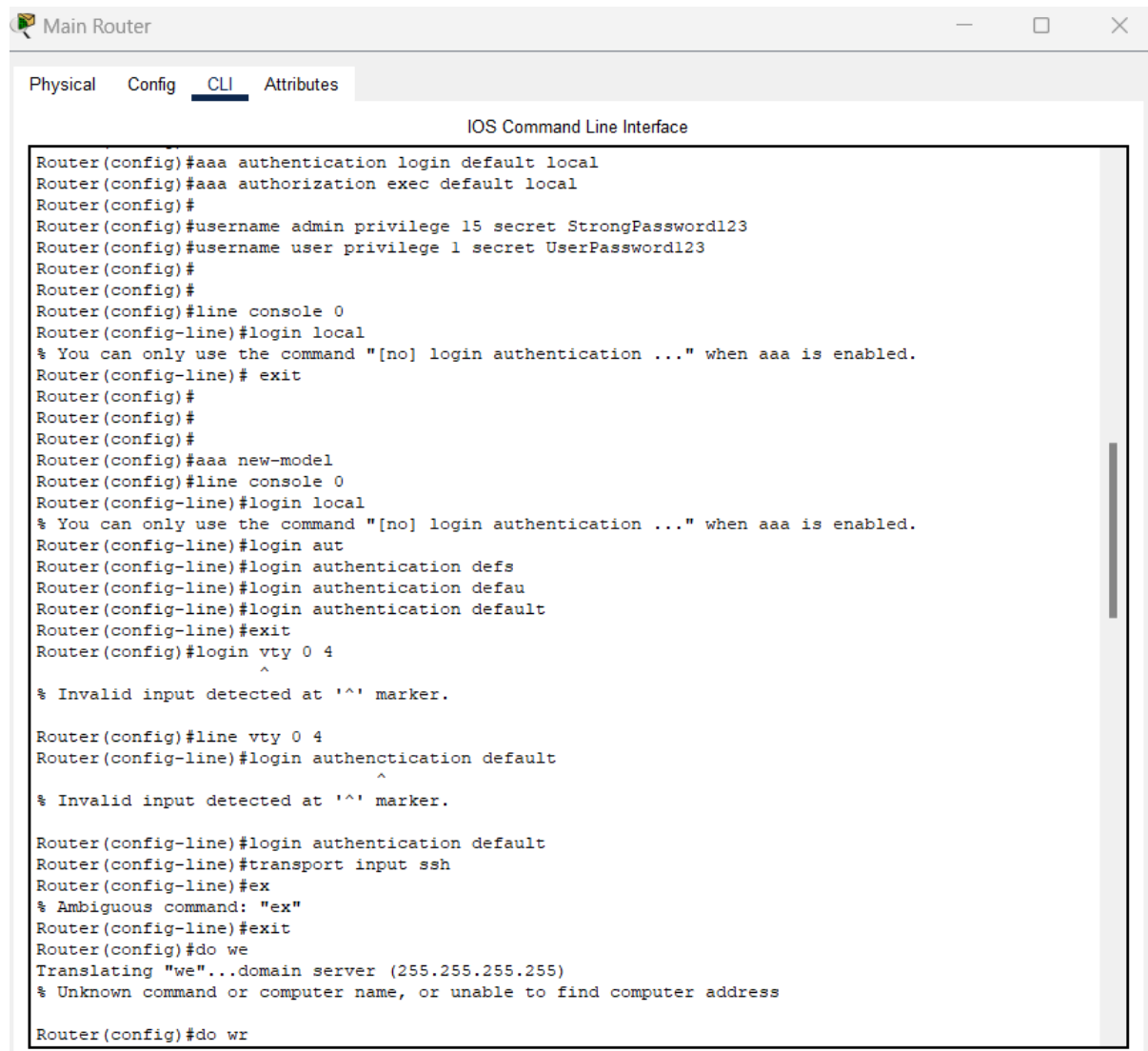


## 4.2 AAA Server Configuration

### Main Router AAA Credentials

username **admin** secret **StrongPassword123**

username **user** secret **UserPassword123**



The screenshot shows a window titled "Main Router" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

```
Router(config)#aaa authentication login default local
Router(config)#aaa authorization exec default local
Router(config)#
Router(config)#username admin privilege 15 secret StrongPassword123
Router(config)#username user privilege 1 secret UserPassword123
Router(config)#
Router(config)#
Router(config)#line console 0
Router(config-line)#login local
% You can only use the command "[no] login authentication ..." when aaa is enabled.
Router(config-line)# exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#aaa new-model
Router(config)#line console 0
Router(config-line)#login local
% You can only use the command "[no] login authentication ..." when aaa is enabled.
Router(config-line)#login aut
Router(config-line)#login authentication defs
Router(config-line)#login authentication defau
Router(config-line)#login authentication default
Router(config-line)#exit
Router(config)#login vty 0 4
      ^
% Invalid input detected at '^' marker.

Router(config)#line vty 0 4
Router(config-line)#login authentication default
      ^
% Invalid input detected at '^' marker.

Router(config-line)#login authentication default
Router(config-line)#transport input ssh
Router(config-line)#ex
% Ambiguous command: "ex"
Router(config-line)#exit
Router(config)#do we
Translating "we"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Router(config)#do wr
```

Figure 32AAA

The AAA authentication and authorization settings are correctly configured using `aaa authentication login default local` and `aaa authorization exec default local`, ensuring that locally stored usernames handle authentication and authorization. The user accounts (admin and user) with different privilege levels are successfully created using `username ... secret`. The `aaa new-model` command is also correctly applied, enabling advanced authentication mechanisms. Additionally, VTY line authentication is correctly associated with `login authentication default`, ensuring secure remote access.

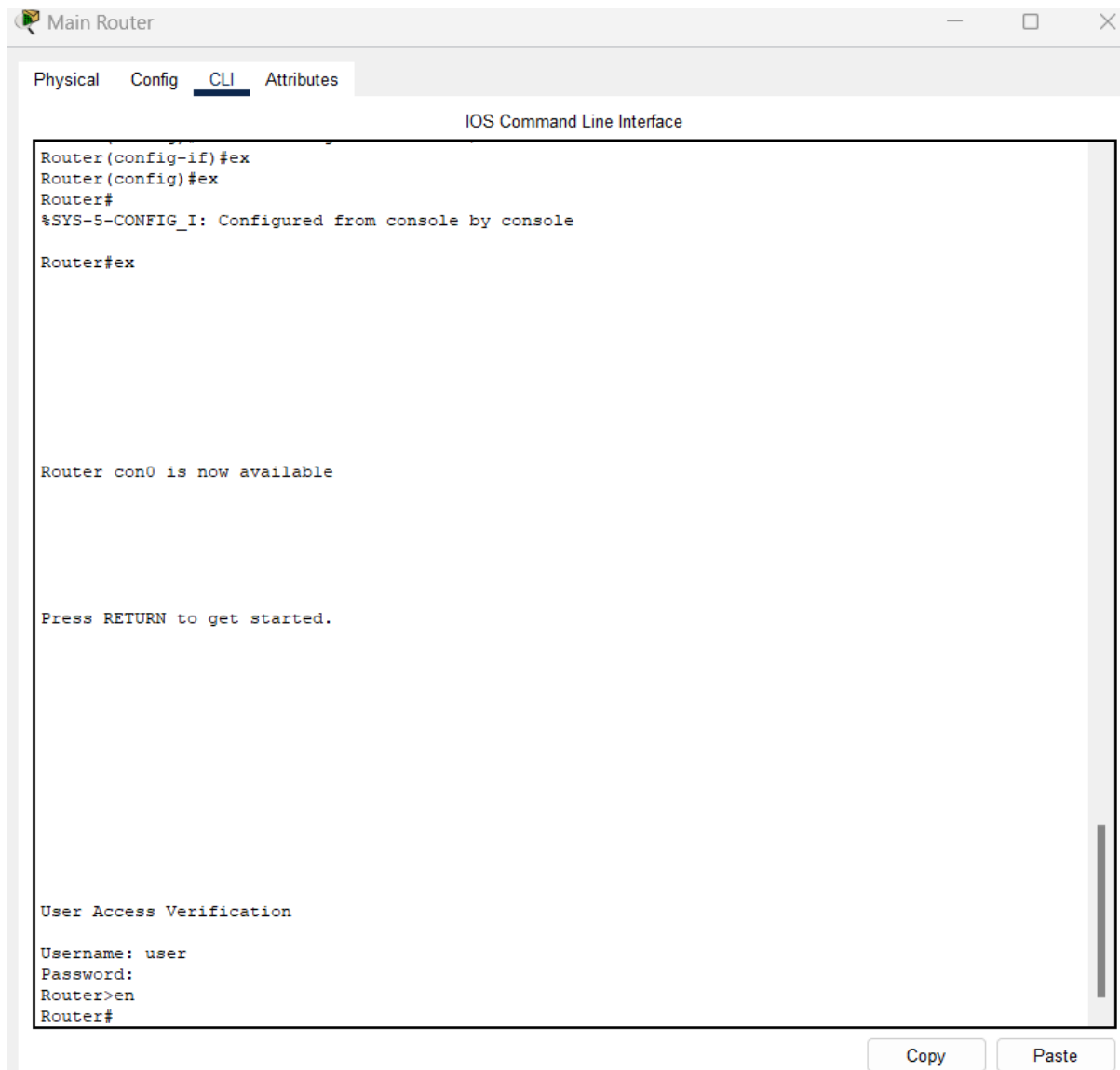


Figure 33AAAPT2

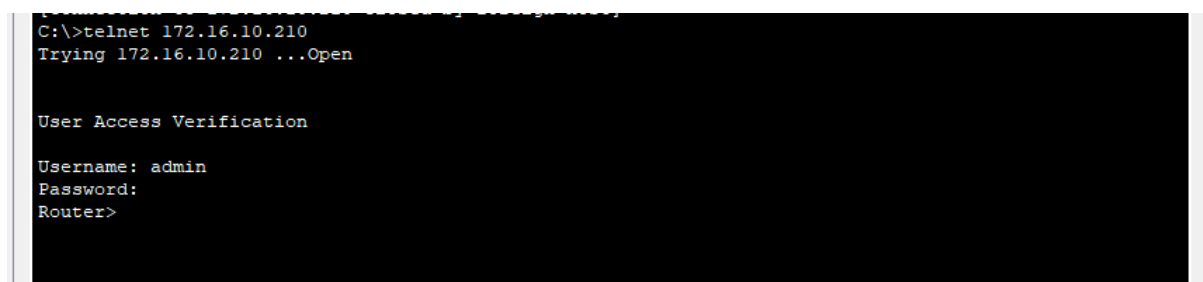


Figure 34AAAPT3

### 4.3 Verification

successful VPN connections and AAA authentication verification is provided in their respective section

## 5. Conclusion

This report outlined the network security design and implementation for Tech Zolutions Inc., focusing on network topology, security zones, and advanced security measures. The router-on-a-stick topology with VLAN segmentation successfully reduced network congestion and enhanced security by isolating departments. A robust IP addressing scheme ensured efficient subnet utilization, while DHCP services provided automated IP allocation. Wireless connectivity was secured with WPA2-PSK, ensuring safe access across all departments.

Security was reinforced through Zones of Trust (Internal, DMZ, and External), with the DMZ hosting web and email servers, preventing direct exposure of internal resources. A Zone-Based Firewall (ZBF) was configured with ACLs and stateful inspection, restricting unauthorized access while allowing necessary services.

A site-to-site VPN using IPsec was deployed between the External Router and Main Router, enabling secure communication between internal and external networks. The VPN encrypted data transmissions, ensuring confidentiality and integrity. AAA authentication was implemented using TACACS+, centralizing user authentication and authorization.

For future improvements, implementing Intrusion Detection/Prevention Systems (IDS/IPS), enabling Multi-Factor Authentication (MFA)