Secure Network Design and Implementation for Tech Zolutions Inc.

A Comprehensive Report on Network Architecture, Security Policies, and Advanced Configurations

Prepared by:

Yash Bhootra

Table Of Contents

1. Introduction

1.1 Purpose of the Report

This report presents a comprehensive network design and security implementation plan for Tech Zolutions Inc., a prominent software development company with 150 employees spread across five departments. The company has recently moved to a new office and requires a secure, scalable, and high-performance network infrastructure to support its daily operations. The primary objective of this report is to analyze, design, configure, and implement an enterprise-level network that adheres to industry best practices in network security, performance optimization, and access control.

In today's rapidly evolving digital landscape, organizations face numerous cybersecurity threats, including unauthorized access, data breaches, and insider attacks. This report goes beyond simply establishing network connectivity and resource allocation, it incorporates multi-layered security mechanisms to protect against both internal and external threats.

1.2 Scope and Objectives

This project covers both the design of the network infrastructure and the implementation of security measures to meet the operational and cybersecurity requirements of Tech Zolutions Inc. The key objectives of this report are as follows:

Network Design & Topology Development

- Develop a structured and scalable hierarchical network topology that aligns with the organization's needs.
- Implement subnetting and VLAN segmentation to optimize network efficiency and improve security.
- Establish secure wireless network access for each department, ensuring controlled connectivity.

Security Implementation & Access Control

- Configure Access Control Lists (ACLs) to enforce network access restrictions and prevent unauthorized communication between departments.
- Deploy a Zone-Based Firewall (ZBF) to regulate inter-departmental network traffic and protect critical assets.
- Implement AAA (Authentication, Authorization, and Accounting) mechanisms using RADIUS or TACACS+ for centralized user authentication and access control.

Advanced Security & Remote Connectivity

- Set up a site-to-site VPN to enable secure communication between the main office and the remote branch.
- Enforce encryption and authentication policies for critical services.

Network Validation & Testing

- Conduct network connectivity tests to verify seamless communication across devices and departments.
- Perform security testing to evaluate the effectiveness of firewall rules, ACLs, and VPN configurations, ensuring compliance with security best practices.

By accomplishing these objectives, the proposed network solution will enhance overall efficiency, security, and scalability, providing a robust foundation for Tech Zolutions Inc. to operate securely and efficiently in the long run.

1.3 Structure of the Report

To ensure clarity and logical progression, this report is structured as follows:

- Section 2: Provides an overview of Tech Zolutions Inc., detailing its departmental requirements and security considerations.
- Section 3: Explains the network design, including topology selection, VLAN segmentation, IP addressing, and OSPF routing configuration.
- Section 4: Discusses the implementation of security measures, focusing on firewalls, ACLs, and network segmentation strategies.
- Section 5: Covers advanced security mechanisms, including VPN configuration and AAA authentication setup.
- Section 6: Concludes with findings and recommendations for potential future improvements.

2. Company Overview and Network Requirements

2.1 About Tech Zolutions Inc.

Tech Zolutions Inc. is a rapidly expanding software development company specializing in enterprise software solutions. The company is structured into five primary departments, each with distinct networking and security needs that must be carefully addressed to ensure operational efficiency and cybersecurity compliance.

Departmental Overview and Network Dependencies

Each department within Tech Zolutions Inc. has specific network access needs and security considerations, as outlined below:

Department	No. of Employees	Primary Network Requirements	Security Considerations
Sales & Marketing	30	Internet access, customer engagement tools, file server access	Prevent unauthorized access to internal resources
Development	50	Limited internet access, access to source code repositories, testing environments	Restrict external connectivity, enforce internal security policies
IT	20	Full administrative access, network and security management	Unrestricted privileged access to all resources
Human Resources (HR)	25	Employee record management, payroll system access	Enforce encryption and access control policies
Finance	25	Online banking, financial record access, secure transactions	Implement strict firewall rules and encrypted communication
Conference Room	-	Video conferencing, internet access only	Isolate from corporate network

Figure 2.1 Department Overview

Dedicated Server Room

Tech Zolutions Inc. also operates a dedicated server room that hosts critical infrastructure components:

- File Server: Stores shared company documents, including marketing materials, employee records, and financial reports.
- Web Server: Hosts internal applications and the company's external-facing website.
- DHCP Server: Assigns dynamic IP addresses to all network devices.
- Email Server: Manages internal and external email communication.

2.2 Departmental Needs and Access Requirements

The network infrastructure must be designed to effectively meet departmental access and security requirements while ensuring optimized traffic flow and resource availability. The following network access model outlines the required access controls:

- Sales & Marketing must have unrestricted access to the internet while being restricted from accessing internal development resources.

- Development should have controlled internet access and privileged access to internal development servers while being restricted from other departmental networks.
- IT must have full administrative control over all network and security infrastructure, ensuring seamless network management.
- HR and Finance must have restricted access to protect confidential and sensitive data, limiting exposure to unauthorized personnel.
- Conference Room must be fully isolated to prevent unauthorized access to corporate resources while allowing internet-based communication.

2.3 Security and Compliance Considerations

A secure and well-structured network infrastructure is essential to mitigate risks such as unauthorized access, data breaches, and cyberattacks. To ensure compliance with security best practices and industry standards, the following security principles and mechanisms will be implemented:

2.3.1 Network Segmentation

- VLAN and subnetting strategies will be used to ensure each department operates within an isolated environment, preventing unauthorized lateral movement of threats across the network.

2.3.2 Access Control Mechanisms

- Access Control Lists (ACLs) will be implemented to enforce strict access rules, preventing unnecessary inter-departmental communication while allowing essential service access.

2.3.3 Firewall and Perimeter Security

- A Zone-Based Firewall (ZBF) will be deployed to segregate network trust zones, ensuring comprehensive traffic inspection and controlled access between different network segments.

2.3.4 VPN and Secure Remote Access

- A site-to-site IPsec VPN will be implemented to securely connect the main office with the remote branch, enabling seamless communication for remote employees.

2.3.5 Encryption and Data Protection

- AAA Authentication Servers (RADIUS/TACACS+) will be utilized to ensure Role-Based Access Control (RBAC) and identity verification for network users, limiting access based on user roles and responsibilities.

Conclusion

By implementing these security measures, Tech Zolutions Inc. will have a robust, resilient, and compliant network architecture that adheres to industry best practices. The proposed design will effectively balance security, performance, and scalability, ensuring that employees can work efficiently while maintaining a high level of data protection and system integrity.

3. Network Design and Configuration

3.1 Network Topology Design

3.1.1 Purpose

A well-structured network topology is critical for ensuring reliable, secure, and efficient communication within an organization. The network topology of Tech Zolutions Inc. has been carefully designed to:

1. Segment the network logically - VLANs are used to separate departments, reducing broadcast domains and improving security.
2. Enable controlled inter-department communication - Using inter-VLAN routing with Access Control Lists (ACLs) to enforce department-based access control.
3. Improve security by isolating critical resources - The server room and conference room are placed in dedicated subnets to prevent unauthorized access.
4. Support future scalability - The hierarchical model ensures additional users, departments, and remote branches can be seamlessly integrated.
5. Optimize network performance - Implementing high-speed cabling and VLAN segmentation reduces latency and network congestion.

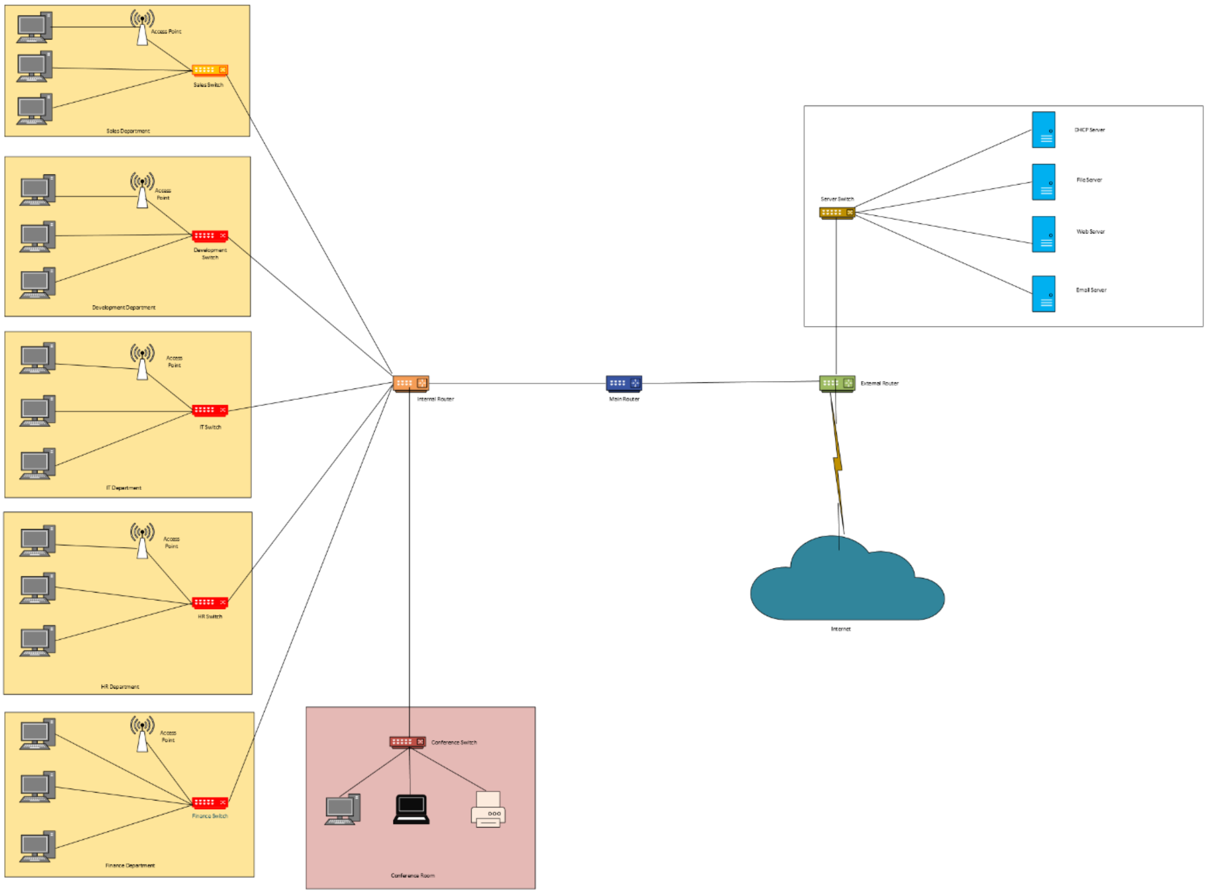


Figure 3.1.1 Network Topology Design

3.1.2 Configuration

The network topology follows the three-tier hierarchical model which ensures modularity, scalability, and performance. The three layers are:

- Core Layer – Connects all major components of the network, including routers and switches.
- Distribution Layer – Implements VLANs, routing, and access control.
- Access Layer – Connects end-user devices (PCs, laptops, printers, Wi-Fi Aps, etc.).

3.1.2.1 Devices Used and Justifications

Device Type	Model Used	Justification
Main Router	Cisco 2911	Manages inter-VLAN routing, OSPF dynamic routing, ACLs, firewall policies, and VPN 8tunnelling. Supports Gigabit Ethernet and VPN encryption.
Internal Router	Cisco 2911	Handles departmental VLANs and inter-VLAN routing for Sales, Development, IT, HR, and Finance. Connected to the Main Router and the Conference Room via dedicated links.
External Router	Cisco 2911	Provides internet access, VPN termination, and firewall enforcement.
Layer 2 Department Switches	Cisco 2960-24TT	Provides 24 Fast Ethernet ports for wired connections, VLAN trunking, and departmental segmentation.
Server Switch	Cisco 2960-24TT	Connects servers (Web, Email, File, and DHCP) securely, ensuring fast data transmission.
Wireless Access Points	Cisco Aironet	Provides Wi-Fi access with separate SSIDs for each department, supporting enterprise WPA2-Enterprise encryption.
End-User Devices	PCs, Laptops, Printers	Devices connected via wired and wireless networks to ensure departmental productivity.

Table 3.1.2.1 List of Devices

3.1.2.2 Cables and Connectivity

Cable Type	Usage	Justification
Copper Crossover	Router-to-Router Connections (Internal Router to Main Router & Conference Room)	It is used because routers are similar devices, requiring crossover connections for direct communication. It ensures high-speed, low-latency communication between internal and main routers.
Copper Straight-Through	PC-to-Switch, Switch-to-Router, Server-to-Switch Connections	It is a standard cable type for connecting different device types, ensuring high-speed data transfer. It provides a stable and interference-free connection for wired users and servers.
Coaxial Cable	ISP Connection (External Router to Internet)	It ensures high-speed broadband connectivity with minimal interference.

Figure 3.1.2.2 Types of Cables

3.2 IP Addressing and Subnetting

3.2.1 Purpose

A structured IP addressing scheme is necessary for:

1. Logical segmentation of departments, ensuring each department has a dedicated subnet.
2. Preventing unnecessary inter-department traffic, reducing congestion and increasing security.
3. Enabling dynamic and static IP allocation, ensuring end-user devices receive IPs dynamically while servers retain static addresses.
4. Optimizing routing and ACLs, allowing restricted access based on subnet policies.

The 172.16.10.0/24 subnet is used as the base network, with specific subnetting for each department.

3.2.2 Subnet Configuration

Department	Subnet Mask	Network Range	Usable Hosts	Broadcast Address	Gateway IP	Subnet Mask
Sales	/26 (255.255.255.192)	172.16.10.0 – 172.16.10.63	62	172.16.10.63	172.16.10.1	/26 (255.255.255.192)
Development	/26 (255.255.255.192)	172.16.10.64 – 172.16.10.127	62	172.16.10.127	172.16.10.65	/26 (255.255.255.192)
IT	/27 (255.255.255.224)	172.16.10.128 – 172.16.10.159	30	172.16.10.159	172.16.10.129	/27 (255.255.255.224)
HR	/27 (255.255.255.224)	172.16.10.160 – 172.16.10.191	30	172.16.10.191	172.16.10.161	/27 (255.255.255.224)
Finance	/27 (255.255.255.224)	172.16.10.192 – 172.16.10.223	30	172.16.10.223	172.16.10.193	/27 (255.255.255.224)
Conference Room	/29 (255.255.255.248)	172.16.10.224 – 172.16.10.231	6	172.16.10.231	172.16.10.225	/29 (255.255.255.248)
Server Room	/29 (255.255.255.248)	172.16.10.232 – 172.16.10.239	6	172.16.10.239	172.16.10.233	/29 (255.255.255.248)

Figure 3.2.2 Subnet Table

3.2.3 Justification for Subnetting Strategy

The subnetting plan for Tech Zolutions Inc. is designed to provide logical network segmentation, efficient IP allocation, enhanced security, and scalability. Below, we got into the detailed justifications for why each subnet was assigned its specific range, subnet mask, and gateway.

3.2.3.1 Logical Departmental Segmentation

Each department is allocated its own subnet to:

- Restrict unnecessary inter-department communication, reducing security risks.
- Minimize broadcast traffic, ensuring efficient data transmission.
- Allow controlled access via ACLs (Access Control Lists), ensuring departments communicate only when necessary.

Additionally:

- Critical infrastructure components such as servers and the conference room are isolated from general user traffic.
- The server room and conference room use /29 subnets, as they have limited devices.
- The main departments use /26 or /27 subnets, ensuring optimal address allocation.

3.2.3.3 Justification for Subnet Sizes

Sales & Development - /26 Subnets (Supports 62 Hosts)

- Sales has 30 employees, and Development has 50, which means a /27 (30 usable hosts) would be insufficient for Development.
- A /26 provides up to 62 usable IPs, allowing future expansion without needing to reconfigure subnet masks.
- Wi-Fi clients, printers, and VoIP phones also require IP addresses, justifying a slightly larger subnet.

IT, HR, Finance – /27 Subnets (Supports 30 Hosts)

- Each of these departments has between 20-25 employees, and a /28 (14 hosts) would be too small.
- A /27 allows 30 usable IPs, which covers:
  1. End-user devices (PCs, laptops, printers).
  2. Departmental Wi-Fi clients.
  3. Any additional network monitoring tools IT may use.
- Security:
  1. HR & Finance need stricter security policies, limiting their exposure to other department networks.
  2. IT needs unrestricted access but should not be part of a larger open subnet for security reasons.

Conference Room & Server Room – /29 Subnets (Supports 6 Hosts)

- The conference room only requires Wi-Fi, a few video conferencing devices, and a single network printer.
- The server room requires dedicated IPs for File, Mail, DHCP and Web server.
- A /29 subnet provides exactly 6 usable IPs, ensuring these critical systems are isolated and secure.
- This subnetting prevents external access to the servers unless explicitly allowed by ACLs.

3.2.3.4 Gateway IP Assignments Justification

Each VLAN is assigned a gateway IP on the Internal Router, ensuring controlled traffic flow.

- We need separate gateway IPs because:
  - Inter-VLAN routing requires each VLAN to have a unique gateway.
  - These gateway IPs allow devices in the VLAN to communicate externally.
  - ACLs on the router can control what traffic is allowed between VLANs.

For example:

- Sales VLAN:
  - Gateway: 172.16.10.1
  - Allows internet & file server access, but blocks access to Finance/HR.
- Finance VLAN:
  - Gateway: 172.16.10.193
  - Blocks unauthorized access from Development, Sales, and Conference Room.

3.2.3.5 Security Benefits of the Subnetting Strategy

The chosen subnetting scheme directly improves network security by:

- Isolating sensitive departments (HR & Finance) from departments with higher internet exposure (Sales & Development).
- Preventing unauthorized inter-departmental traffic, enforced using firewall rules and ACLs.
- Minimizing the impact of a security breach - if a device in one VLAN is compromised, the attack is contained within that subnet.
- Ensuring better monitoring and logging - Each department's traffic is logged separately, helping IT track anomalies.

3.2.3.6 Scalability

The subnetting plan allows for future growth in multiple ways:

- Sales and Development were given /26 subnets, meaning they have space for additional users without requiring re-subnetting.
- Each subnet has additional unused IPs to accommodate:
    - New employees.
    - Additional Wi-Fi-enabled devices.
    - Expansion of department-specific applications.

3.2.3.7 Network Performance Optimization

- Minimizes broadcast domains:
    - A /24 network with 150+ devices would lead to unnecessary broadcast traffic.
    - Breaking it down into smaller subnets (e.g., /26, /27, /29) limits broadcast storms.
- Reduces congestion & increases efficiency:
    - Departments handling resource-intensive tasks (Development & Finance) get their own subnets, preventing slowdowns from network-wide traffic.

3.3 Network Device Configuration and VLAN Implementation

3.3.1 Purpose

The purpose of this section is to configure all network devices with the appropriate settings to ensure optimal functionality, security, and efficiency. The configurations involve:

1. Configuring essential routing protocols such as OSPF to enable efficient dynamic routing between VLANs and external networks.
2. Implementing VLANs on switches to logically segment departmental traffic and improve network performance and security.

3. Configuring network interfaces on routers and switches to ensure proper communication between departments, servers, and the external network.

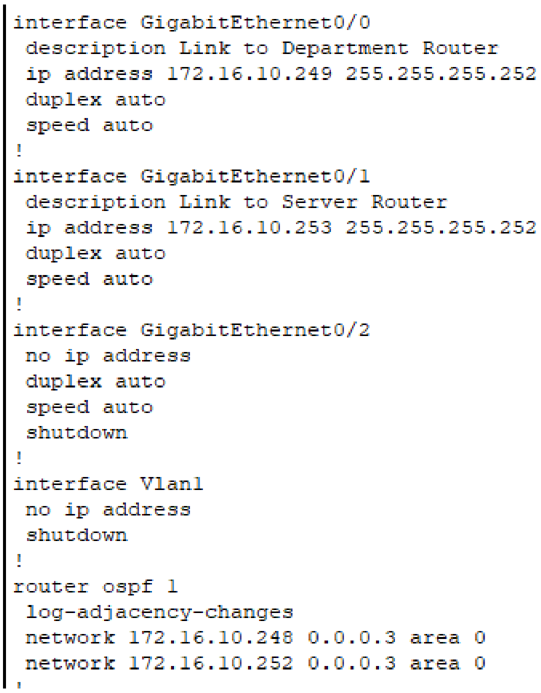
4. Setting up DHCP services to enable automatic IP address assignment.

5. Setting up Access points around department rooms.

3.3.2 Configuration of Network Devices

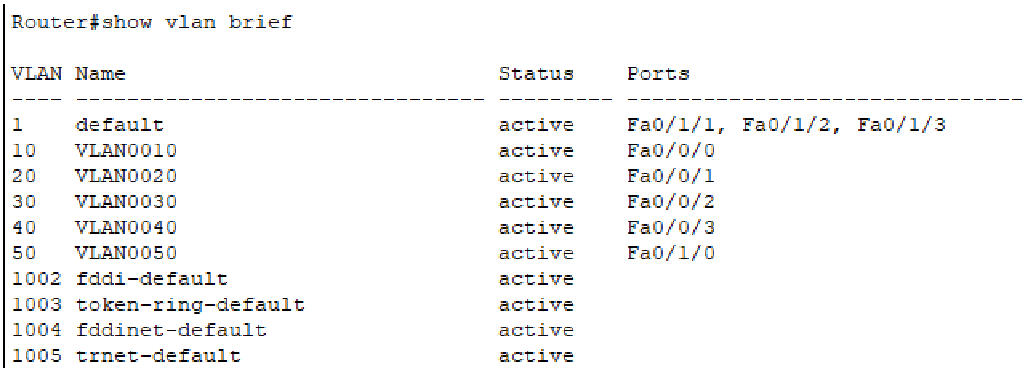
The network is structured in a hierarchical model, ensuring modularity, scalability, and security. Each department is assigned a VLAN, and routing is handled by a dedicated interface on the router.

➔ **Configuring Router Interfaces and OSPF for Dynamic Routing:**



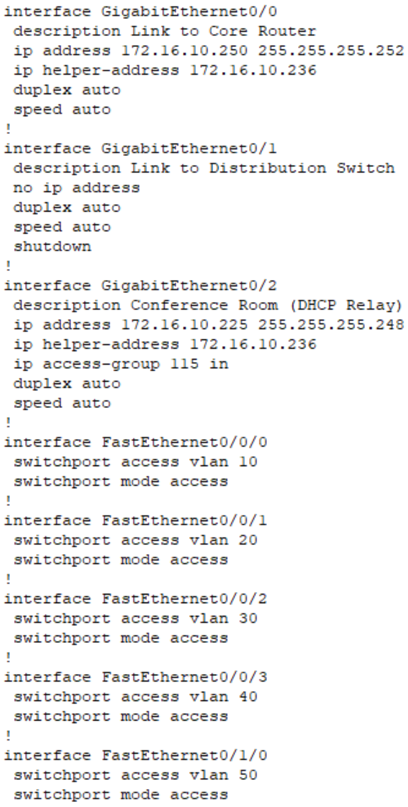
```
interface GigabitEthernet0/0
 description Link to Department Router
 ip address 172.16.10.249 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description Link to Server Router
 ip address 172.16.10.253 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 172.16.10.248 0.0.0.3 area 0
 network 172.16.10.252 0.0.0.3 area 0
!
```

Figure: Main Router Interfaces



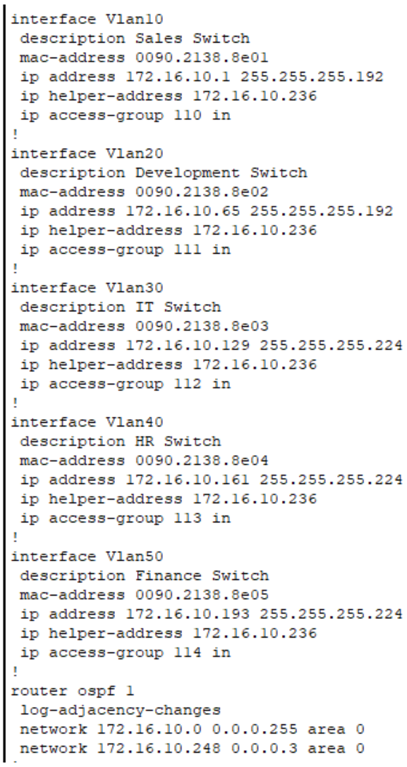
```
Router#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1/1, Fa0/1/2, Fa0/1/3
10   VLAN0010                         active    Fa0/0/0
20   VLAN0020                         active    Fa0/0/1
30   VLAN0030                         active    Fa0/0/2
40   VLAN0040                         active    Fa0/0/3
50   VLAN0050                         active    Fa0/1/0
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure: Internal Router VLAN Configuration



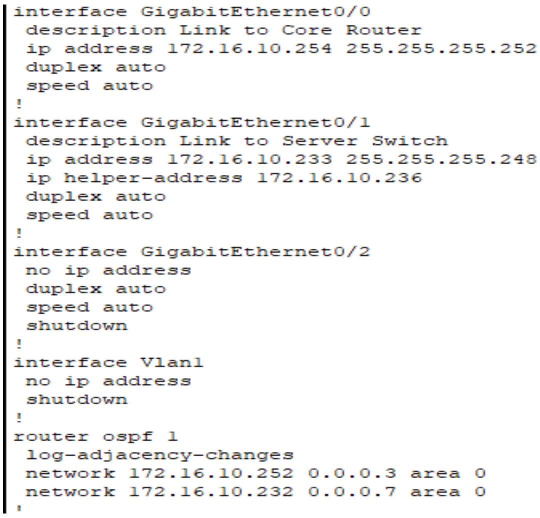
```
interface GigabitEthernet0/0
 description Link to Core Router
 ip address 172.16.10.250 255.255.255.252
 ip helper-address 172.16.10.236
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description Link to Distribution Switch
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 description Conference Room (DHCP Relay)
 ip address 172.16.10.225 255.255.255.248
 ip helper-address 172.16.10.236
 ip access-group 115 in
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/0/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/0/3
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/1/0
 switchport access vlan 50
 switchport mode access
```

Figure: Internal Router Interfaces 1



```
interface Vlan10
 description Sales Switch
 mac-address 0090.2138.8e01
 ip address 172.16.10.1 255.255.255.192
 ip helper-address 172.16.10.236
 ip access-group 110 in
!
interface Vlan20
 description Development Switch
 mac-address 0090.2138.8e02
 ip address 172.16.10.65 255.255.255.192
 ip helper-address 172.16.10.236
 ip access-group 111 in
!
interface Vlan30
 description IT Switch
 mac-address 0090.2138.8e03
 ip address 172.16.10.129 255.255.255.224
 ip helper-address 172.16.10.236
 ip access-group 112 in
!
interface Vlan40
 description HR Switch
 mac-address 0090.2138.8e04
 ip address 172.16.10.161 255.255.255.224
 ip helper-address 172.16.10.236
 ip access-group 113 in
!
interface Vlan50
 description Finance Switch
 mac-address 0090.2138.8e05
 ip address 172.16.10.193 255.255.255.224
 ip helper-address 172.16.10.236
 ip access-group 114 in
!
router ospf 1
 log-adjacency-changes
 network 172.16.10.0 0.0.0.255 area 0
 network 172.16.10.248 0.0.0.3 area 0
```

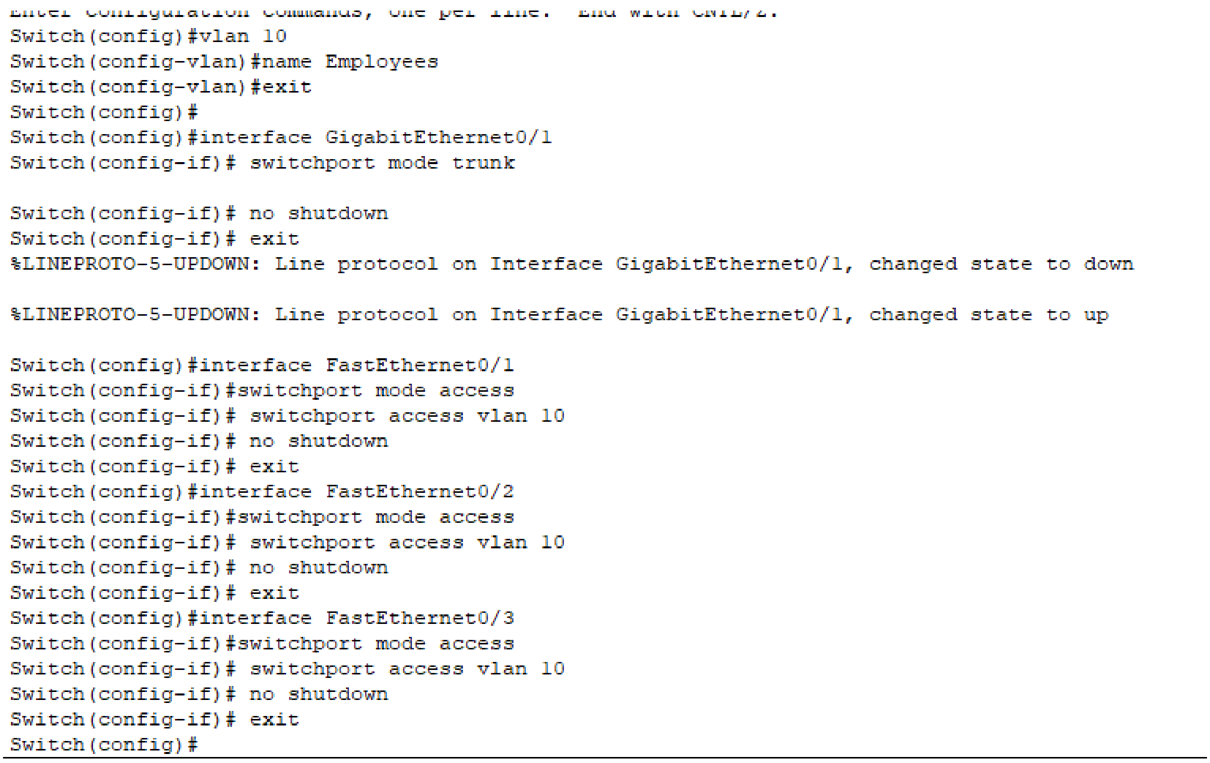
Figure: Internal Router VLAN Interfaces and OSPF



```
interface GigabitEthernet0/0
 description Link to Core Router
 ip address 172.16.10.254 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description Link to Server Switch
 ip address 172.16.10.233 255.255.255.248
 ip helper-address 172.16.10.236
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 172.16.10.252 0.0.0.3 area 0
 network 172.16.10.232 0.0.0.7 area 0
!
```

Figure: External Router Interfaces and OSPF

➔ **Configuring L2 Switches (Departments, Conference and Server):**



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Employees
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk

Switch(config-if)# no shutdown
Switch(config-if)# exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)#
```

Figure: Sales Switch Configuration

Just like this switch all the other switches has been configured using same concept and commands.

3.3.3 Justification

1. Use of VLANs:

    - Enhances security by preventing unauthorized access between departments.
    - Reduces network congestion by limiting broadcast domains.
    - Improves scalability by allowing easy expansion.

2. Use of Dedicated Router Interfaces Instead of Router-on-a-Stick:

    - Improved performance – No single interface is overloaded with multiple VLANs.
    - Simpler configuration – Each VLAN has a dedicated physical link, reducing complexity.

3. Use of OSPF:

    - Faster convergence in case of network changes.
    - Supports large networks with dynamic route updates.
    - Ensures optimal path selection.

3.4 DHCP Server Configuration

3.4.1 Purpose

The Dynamic Host Configuration Protocol (DHCP) server is an essential component of Tech Zolutions Inc.'s network, responsible for automatically assigning IP addresses to devices within the network. The key objectives of implementing a DHCP server are:

1. Automate IP Address Assignment - Ensures that devices receive an IP address dynamically without manual configuration.

2. Minimize Configuration Errors - Reduces the chance of duplicate IP addresses and misconfigurations.

3. Improve Network Management - DHCP centralizes IP management, making it easier to control address allocation and lease duration.

4. Enhance Scalability - Supports future expansion by dynamically handling IP address distribution without requiring manual intervention.

5. Ensure Consistency - All devices within a subnet receive consistent default gateway, subnet mask, and DNS settings.

3.4.2 DHCP Server Configuration

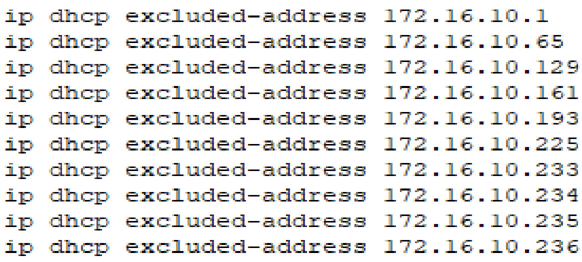
The DHCP server is located in the Server room with a static IP of 172.16.10.236. The DHCP service provides IP addresses dynamically to all VLANs, except for servers, which are assigned static IPs.

3.4.2.1 DHCP Server Setup

The DHCP service is configured on a dedicated server in the Server room to provide IP addresses dynamically to client devices.

Step 1: Excluding Static IP Ranges

Some addresses are reserved for static assignment to servers, routers, and network infrastructure.

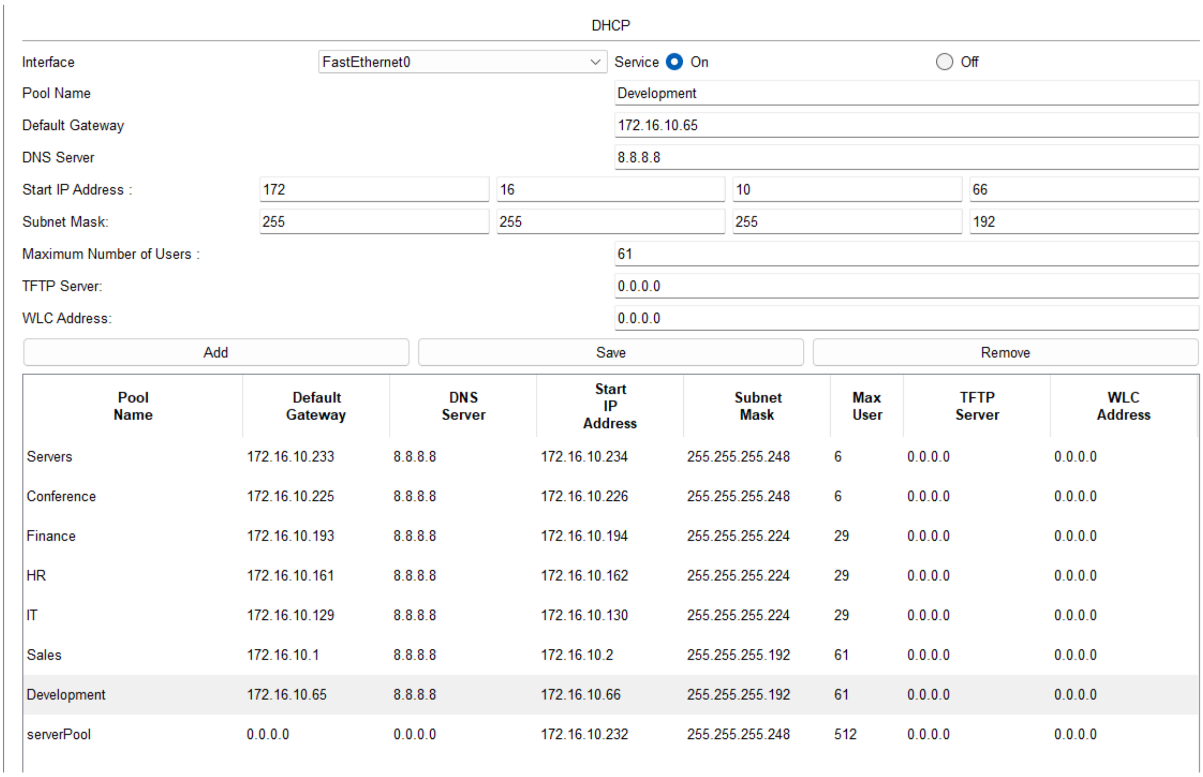


```
ip dhcp excluded-address 172.16.10.1
ip dhcp excluded-address 172.16.10.65
ip dhcp excluded-address 172.16.10.129
ip dhcp excluded-address 172.16.10.161
ip dhcp excluded-address 172.16.10.193
ip dhcp excluded-address 172.16.10.225
ip dhcp excluded-address 172.16.10.233
ip dhcp excluded-address 172.16.10.234
ip dhcp excluded-address 172.16.10.235
ip dhcp excluded-address 172.16.10.236
```

Figure: Excluded DHCP IP's

Step 2: Configuring DHCP Pools for Each VLAN

Each VLAN is assigned a dedicated DHCP pool, ensuring that devices within each department receive the correct subnet and gateway.



DHCP

Interface: FastEthernet0

Service ● On ○ Off

Pool Name: Development

Default Gateway: 172.16.10.65

DNS Server: 8.8.8.8

Start IP Address : 172 16 10 66

Subnet Mask: 255 255 255 192

Maximum Number of Users : 61

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
Servers	172.16.10.233	8.8.8.8	172.16.10.234	255.255.255.248	6	0.0.0.0	0.0.0.0
Conference	172.16.10.225	8.8.8.8	172.16.10.226	255.255.255.248	6	0.0.0.0	0.0.0.0
Finance	172.16.10.193	8.8.8.8	172.16.10.194	255.255.255.224	29	0.0.0.0	0.0.0.0
HR	172.16.10.161	8.8.8.8	172.16.10.162	255.255.255.224	29	0.0.0.0	0.0.0.0
IT	172.16.10.129	8.8.8.8	172.16.10.130	255.255.255.224	29	0.0.0.0	0.0.0.0
Sales	172.16.10.1	8.8.8.8	172.16.10.2	255.255.255.192	61	0.0.0.0	0.0.0.0
Development	172.16.10.65	8.8.8.8	172.16.10.66	255.255.255.192	61	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.16.10.232	255.255.255.248	512	0.0.0.0	0.0.0.0

Figure: DHCP Pool

Since the DHCP server is in Server room which is connected to external router, DHCP relay agents are configured on all VLAN interfaces to forward DHCP requests.

3.4.3 Justification for DHCP Implementation

1. Use of Centralized DHCP Server:

- Easier IP Management - Instead of configuring static IPs on each device, DHCP automates assignments.

- Prevents IP Conflicts - Ensures each device gets a unique IP address, avoiding duplicate address issues.

2. Configure DHCP Relay on the Router:

- DHCP traffic is broadcast-based, meaning requests from other VLANs would not reach the DHCP server without a relay.
- The router forwards requests to the DHCP server, ensuring clients in different VLANs receive IP addresses correctly.

3. Excluding Static IPs for Servers:

- Servers require fixed IPs so that devices can always connect reliably.
- If a server's IP changes, client devices may fail to locate services like email, file sharing, and web hosting.
- Predefined ACLs and firewall rules rely on consistent server IPs.

4. Assigning Unique VLANs for Each Department:

- Ensures segmentation of traffic, improving security and performance.
- Allows the DHCP server to allocate IPs specific to each department, preventing address conflicts.

3.5 Wireless Network Setup

3.5.1 Purpose

The implementation of wireless networks in Tech Zolutions Inc. is crucial for providing seamless mobility, accessibility, and efficiency within the organization. The primary objectives of the wireless network setup are:

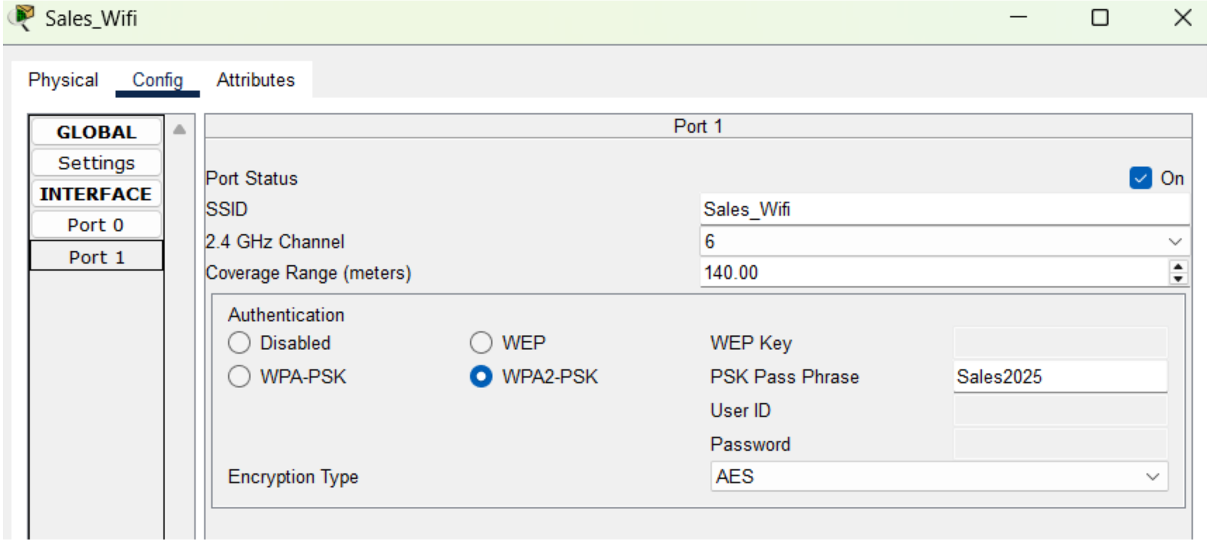
1. Provide Secure Wireless Access - Ensure each department has its own secure Wi-Fi network to prevent unauthorized access.
2. Enable Mobility for Employees - Employees can move freely without losing connectivity.
3. Support Guest Access & Conference Room Wi-Fi - A separate guest network is provided in the conference room isolated from internal resources.
4. Implement WPA2/3 Security - Prevent unauthorized access and data interception using strong encryption.
5. Optimize Wireless Performance - Ensure minimum interference and maximum coverage with proper channel selection and power adjustments.

3.5.2 Wireless Network Configuration

The wireless network is implemented using enterprise-grade access points to provide reliable connectivity with proper security policies.

SSID	VLAN ID	Subnet Assigned	Purpose	Security Type	Password
Sales_WiFi	10	172.16.10.0/26	Wireless access for Sales	WPA2-Enterprise	Sales2025
Development_WiFi	20	172.16.10.64/26	Wireless access for Developers	WPA2-Enterprise	Development2025
IT_WiFi	30	172.16.10.128/27	Secure access for IT team	WPA2-Enterprise	ITdev2025
HR_WiFi	40	172.16.10.160/27	Wireless access for HR	WPA2-Enterprise	HRdev2025
Finance_WiFi	50	172.16.10.192/27	Wireless access for Finance	WPA2-Enterprise	Finance2025

Figure 3.5: Access Point Configuration


Sales_Wifi

Port 1

Port Status ☑ On

SSID: Sales_Wifi

2.4 GHz Channel: 6

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: Sales2025

User ID:

Password:

Encryption Type: AES

Figure: Sales AP Configuration

All the access points have been configured using Figure 3.5

3.6 Connectivity Verification

3.6.1 Purpose

After configuring the network topology, VLANs, routing, DHCP, NAT, and wireless networks, it is crucial to verify end-to-end connectivity. The objectives of connectivity verification include:

1. Ensure all VLANs have proper routing and interconnectivity.

2. Verify DHCP-assigned IPs to client devices.

3. Confirm internet access through NAT for internal users.

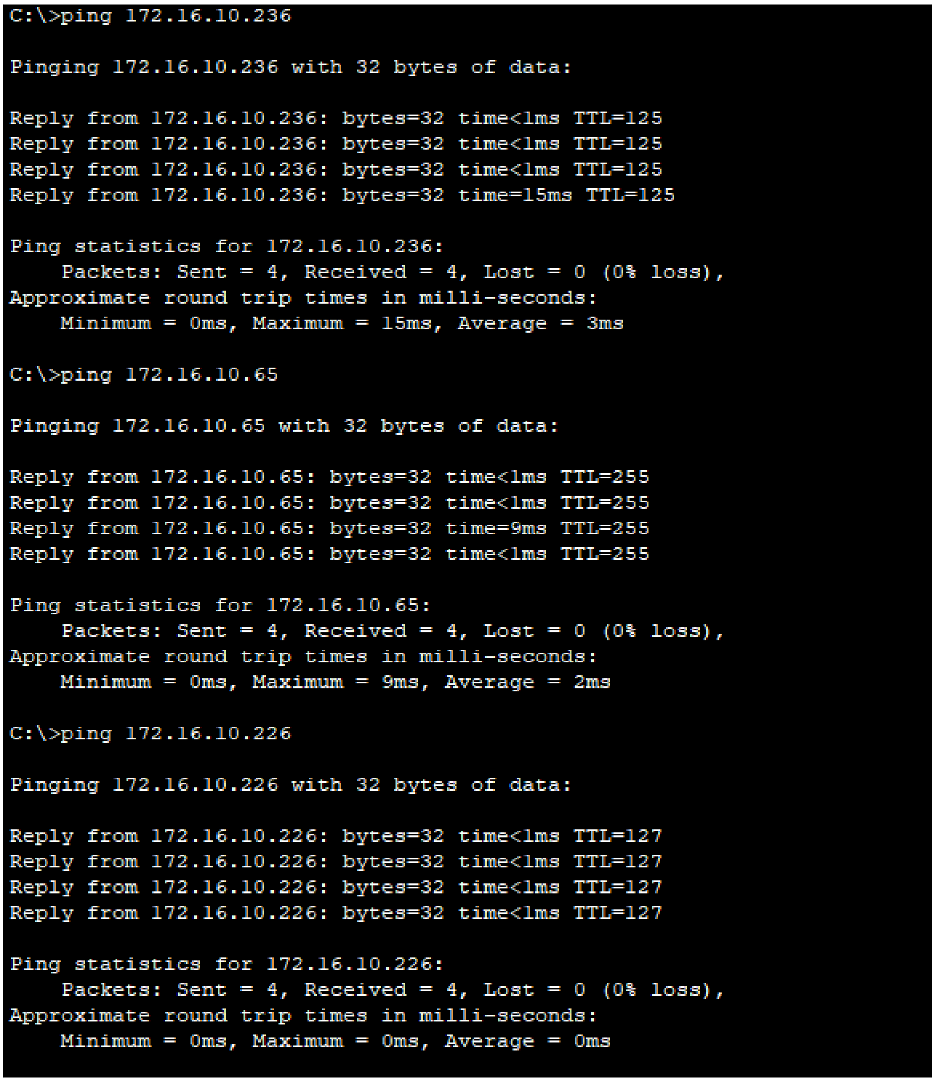
4. Validate secure wireless connectivity for each department.

5. Test firewall and ACL rules to ensure security policies are enforced.

3.6.2 Connectivity Verification Tests

3.7.2.1 VLAN Connectivity Test (Ping Between Departments)

Each VLAN should be able to communicate only with permitted networks.



```
C:\>ping 172.16.10.236

Pinging 172.16.10.236 with 32 bytes of data:

Reply from 172.16.10.236: bytes=32 time<1ms TTL=125
Reply from 172.16.10.236: bytes=32 time<1ms TTL=125
Reply from 172.16.10.236: bytes=32 time<1ms TTL=125
Reply from 172.16.10.236: bytes=32 time=15ms TTL=125

Ping statistics for 172.16.10.236:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms

C:\>ping 172.16.10.65

Pinging 172.16.10.65 with 32 bytes of data:

Reply from 172.16.10.65: bytes=32 time<1ms TTL=255
Reply from 172.16.10.65: bytes=32 time<1ms TTL=255
Reply from 172.16.10.65: bytes=32 time=9ms TTL=255
Reply from 172.16.10.65: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.10.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>ping 172.16.10.226

Pinging 172.16.10.226 with 32 bytes of data:

Reply from 172.16.10.226: bytes=32 time<1ms TTL=127
Reply from 172.16.10.226: bytes=32 time<1ms TTL=127
Reply from 172.16.10.226: bytes=32 time<1ms TTL=127
Reply from 172.16.10.226: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure: Connectivity test from Sales Department PC

As seen in above figure sales PC can ping DHCP server, Development PC and Conference PC which proves proper connectivity around the network.

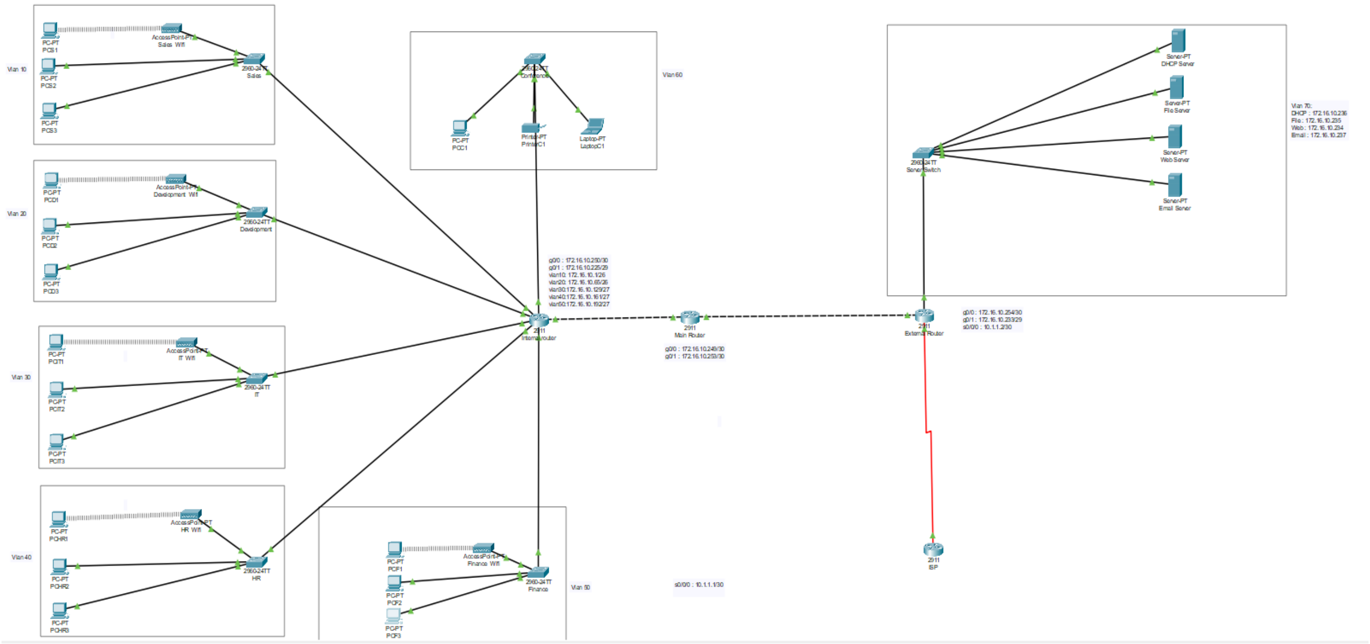


Figure: Packet Tracer Diagram

The above figure shows the network topology in packet tracer after configuring all the devices.

4. Security and Zones of Trust

4.1 Security Configuration on Network Devices

4.1.1 Purpose

The implementation of robust security configurations on network devices is essential to protect the integrity, confidentiality, and availability of Tech Zolutions Inc.'s network infrastructure. The primary security objectives include:

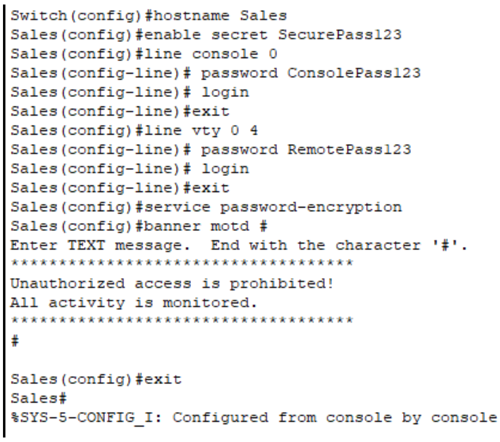
1. Prevent Unauthorized Access - Ensure only authorized personnel can access network devices through secure authentication mechanisms.
2. Mitigate Network Attacks - Protect against threats such as brute-force attacks, unauthorized device connections, and MAC spoofing.
3. Secure Management Access - Implement encrypted remote management protocols to prevent credential theft.
4. Limit Physical Attack Vectors - Disable unused interfaces and implement port security to prevent rogue device connections.
5. Ensure Device Hardening - Secure routers and switches by disabling unused services, enabling strong password policies, and encrypting stored passwords.

4.1.2 Security Hardening of Routers and Switches

Security hardening is applied to all network devices including routers, switches, and access points to protect against internal and external threats. Figure below shows the configurations applies to all the devices.

Every device have the same below configurations :

a. Secret Password – SecurePass123
b. Console Password – ConsolePass123
c. VTY – RemotePass123



```
Switch(config)#hostname Sales
Sales(config)#enable secret SecurePass123
Sales(config)#line console 0
Sales(config-line)# password ConsolePass123
Sales(config-line)# login
Sales(config-line)#exit
Sales(config)#line vty 0 4
Sales(config-line)# password RemotePass123
Sales(config-line)# login
Sales(config-line)#exit
Sales(config)#service password-encryption
Sales(config)#banner motd #
Enter TEXT message.  End with the character '#'.
************************************
Unauthorized access is prohibited!
All activity is monitored.
************************************
#

Sales(config)#exit
Sales#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 4.1.2: Secure authentication and Console security on Sales Switch

4.1.2.1 Configuring Secure Authentication and Password Protection

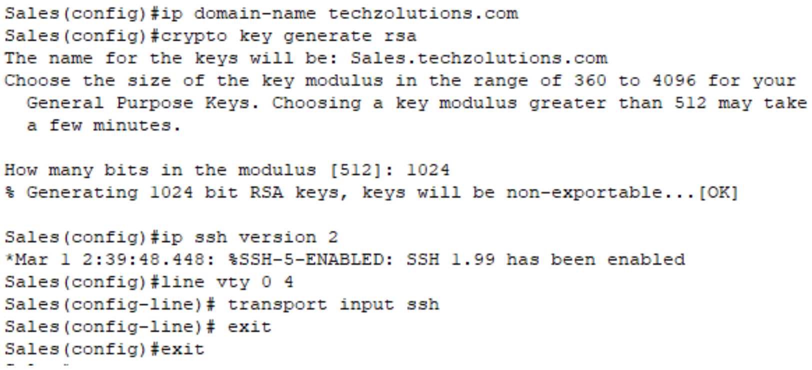
By default, passwords on Cisco devices are stored in plaintext, making them vulnerable to unauthorized access. To enhance security, the enable password is encrypted and strong authentication mechanisms are applied (Figure 4.1.2).

4.1.2.2 Configuring Strong Console and VTY Line Security

By default, console and VTY (virtual terminal) lines do not require authentication, leaving devices exposed to unauthorized logins. To strengthen access control, authentication is enforced (Figure 4.1.2).

4.1.2.3 Secure Remote Management Using SSH (Replacing Telnet)

Telnet transmits passwords in plaintext, making it highly insecure. Instead, SSH (Secure Shell) is configured to encrypt remote administrative access. Same concept and commands have been used on all the devices just like below figure.

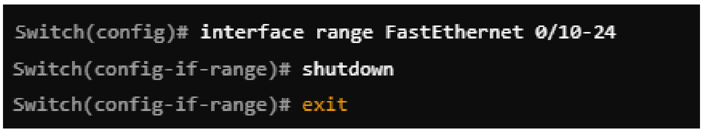


```
Sales(config)#ip domain-name techzolutions.com
Sales(config)#crypto key generate rsa
The name for the keys will be: Sales.techzolutions.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Sales(config)#ip ssh version 2
*Mar 1 2:39:48.448: %SSH-5-ENABLED: SSH 1.99 has been enabled
Sales(config)#line vty 0 4
Sales(config-line)# transport input ssh
Sales(config-line)# exit
Sales(config)#exit
```

Figure 4.1.3: SSH Implementation on Sales Switch

4.1.2.4 Disabling Unused Interfaces on Switches and Routers

To prevent unauthorized physical access, all unused switch ports are shut down on all switches and routers.



```
Switch(config)# interface range FastEthernet 0/10-24
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
```

Figure: Disabling Unused Interfaces on Sales Switch

Security Measure	Justification
SSH for Remote Access	Encrypts management traffic, preventing password exposure
Console & VTY Security	Ensures only authorized users can access network devices.
Disabling Unused Ports	Eliminates potential entry points for unauthorized access.

Figure: Summary of Security Configurations and Justifications

4.2 Zone-Based Firewall (ZPF) Implementation

4.2.1 Purpose

A Zone-Based Firewall (ZPF) is implemented on the Main Router of Tech Zolutions Inc. to enhance network security, traffic filtering, and access control. Unlike traditional access control lists (ACLs), a ZPF provides stateful traffic inspection, ensuring only legitimate, bidirectional communications are allowed between network segments.

The primary objectives of ZPF implementation are:

1. Protecting internal resources by filtering inbound and outbound traffic based on security policies.
2. Restricting unauthorized communication between network zones to prevent lateral movement of threats.
3. Providing stateful packet inspection (SPI) for better security over standard ACLs.
4. Enhancing performance by reducing the number of access control rules required.
5. Ensuring secure external access while blocking malicious or unnecessary traffic.

4.2.2 Defining Security Zones in ZPF

A Zone-Based Firewall (ZPF) divides the network into security zones where each zone represents a logical area of trust.

Security Zone	Description	Network Segments Included
IN (Trusted Zone)	Represents internal users and departmental networks	Sales, Development, IT, HR, Finance VLANs
OUT (Untrusted Zone)	Represents external, untrusted traffic	Internet (ISP-facing interface)
DMZ (Demilitarized Zone)	Contains externally accessible servers	Web Server, Email Server, DHCP Server

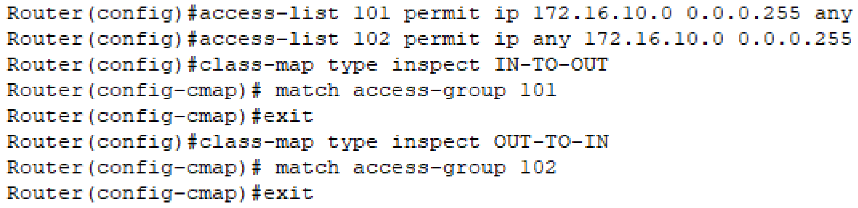
Figure: Security Zones of Main Router

4.2.3 Zone-Based Firewall Configuration Steps

The ZPF implementation on the Main Router follows these key steps:

Step 1: Creating Access Control Lists (ACLs) for Allowed Traffic and Creating Firewall Class Maps

Before defining security zones, ACLs are created to specify which types of traffic are permitted. Class maps define what type of traffic should be inspected in the firewall policies.



```
Router(config)#access-list 101 permit ip 172.16.10.0 0.0.0.255 any
Router(config)#access-list 102 permit ip any 172.16.10.0 0.0.0.255
Router(config)#class-map type inspect IN-TO-OUT
Router(config-cmap)# match access-group 101
Router(config-cmap)#exit
Router(config)#class-map type inspect OUT-TO-IN
Router(config-cmap)# match access-group 102
Router(config-cmap)#exit
```

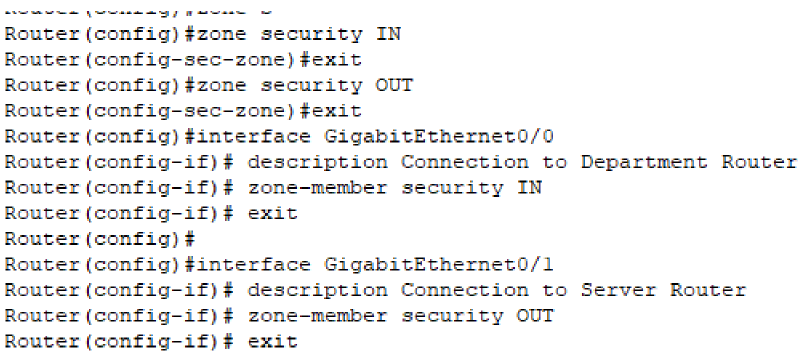
Figure: Access-list and Firewall Class Map

- ACL 101 allows internal devices to initiate outbound traffic.
  ACL 102 allows returning traffic from the internet back into the internal network.

- Class map IN-TO-OUT applies ACL 101 to track outbound connections.
  Class map OUT-TO-IN applies ACL 102 to track return traffic.

Step 2: Defining Security Zones and Assigning Interfaces to Security Zones

Security zones are defined to segment traffic flows. Each interface on the Main Router is assigned to a security zone.



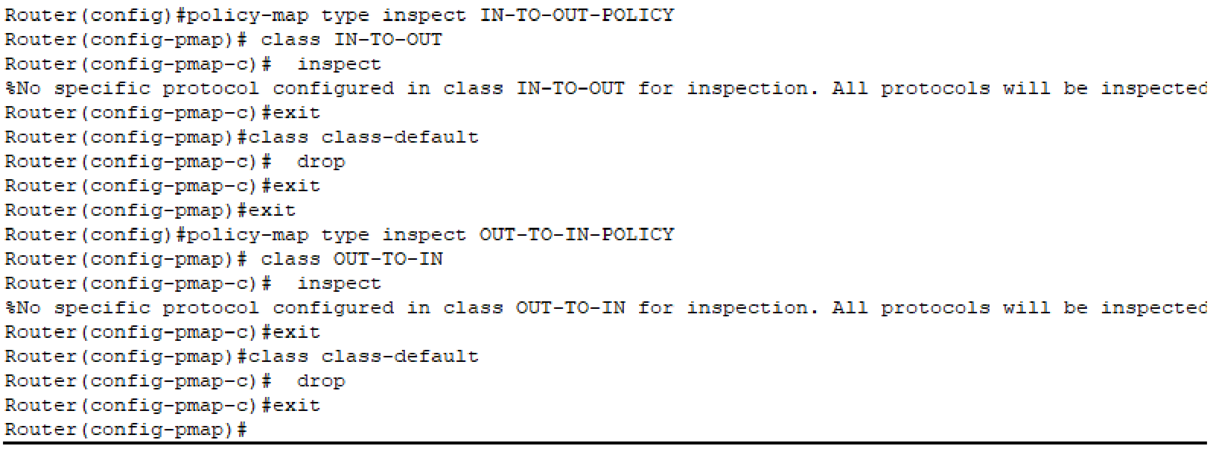
```
Router(config)#zone security IN
Router(config-sec-zone)#exit
Router(config)#zone security OUT
Router(config-sec-zone)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)# description Connection to Department Router
Router(config-if)# zone-member security IN
Router(config-if)# exit
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)# description Connection to Server Router
Router(config-if)# zone-member security OUT
Router(config-if)# exit
```

Figure: Defining Security Zones

- Two zones are created: IN for trusted internal networks and OUT for the untrusted external network.
- The GigabitEthernet0/0 interface (internal network) is assigned to the IN zone.
- The GigabitEthernet0/1 interface (external ISP connection) is assigned to the OUT zone.

Step 3: Creating Policy Maps for Stateful Traffic Inspection

Policy maps define how different classes of traffic should be handled.



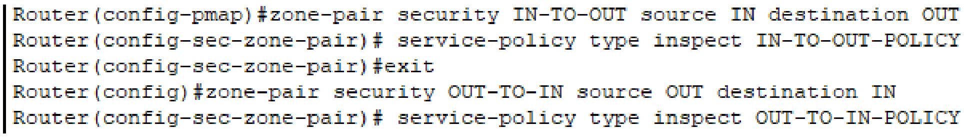
```
Router(config)#policy-map type inspect IN-TO-OUT-POLICY
Router(config-pmap)# class IN-TO-OUT
Router(config-pmap-c)#  inspect
%No specific protocol configured in class IN-TO-OUT for inspection. All protocols will be inspected
Router(config-pmap-c)#exit
Router(config-pmap)#class class-default
Router(config-pmap-c)#  drop
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#policy-map type inspect OUT-TO-IN-POLICY
Router(config-pmap)# class OUT-TO-IN
Router(config-pmap-c)#  inspect
%No specific protocol configured in class OUT-TO-IN for inspection. All protocols will be inspected
Router(config-pmap-c)#exit
Router(config-pmap)#class class-default
Router(config-pmap-c)#  drop
Router(config-pmap-c)#exit
Router(config-pmap)#
```

Figure: Policy Maps

- IN-TO-OUT-POLICY allows and inspects outbound traffic while blocking all other traffic by default.
- OUT-TO-IN-POLICY allows return traffic from the internet and blocks all other inbound connections.

Step 4: Applying Security Policies to Zone Pairs

The final step is to link the security policies to traffic flows between security zones.



```
Router(config-pmap)#zone-pair security IN-TO-OUT source IN destination OUT
Router(config-sec-zone-pair)# service-policy type inspect IN-TO-OUT-POLICY
Router(config-sec-zone-pair)#exit
Router(config)#zone-pair security OUT-TO-IN source OUT destination IN
Router(config-sec-zone-pair)# service-policy type inspect OUT-TO-IN-POLICY
```

Figure: Applying Security Policies to Zone Pairs

- Traffic from IN to OUT is inspected using IN-TO-OUT-POLICY.
- Traffic from OUT to IN is inspected using OUT-TO-IN-POLICY.

4.2.4 Justification for Zone-Based Firewall (ZPF) Implementation

Security Feature	Justification
Stateful Inspection	Unlike ACLs, ZPF tracks active connections and allows return traffic dynamically.
Zone-Based Traffic Control	Ensures security by applying specific policies to different network segments.
Prevention of Unauthorized Access	Ensures internal resources are protected from external attacks.
Policy-Based Management	Simplifies firewall rule management by organizing traffic into class maps and policy maps.
Blocks Unwanted or Malicious Traffic	All traffic is denied by default unless explicitly permitted through security policies.
Granular Traffic Control	Enables precise filtering of protocols, source, and destination traffic flows.
Protects Internal Departments	Prevents direct communication between VLANs without inspection, mitigating internal threats.

Figure: Justification For ZPF implementation

4.3 Access Control Lists (ACLs) Implementation

4.3.1 Purpose of ACL Implementation

Access Control Lists (ACLs) are a crucial component in securing and controlling network traffic. ACLs define rules that filter and restrict access based on source IP, destination IP, and protocols, ensuring that only authorized devices and users can communicate. The key objectives of implementing ACLs in Tech Zolutions Inc. include:

1. Restricting Inter-Department Communication – Ensuring departments can only access required resources.
2. Blocking Unauthorized External Access – Preventing internet hosts from directly accessing internal VLANs.
3. Protecting Critical Servers – Restricting access to DHCP, Web, File, and Email servers.
4. Preventing Malicious Activities – Blocking unauthorized ICMP traffic and lateral movement.
5. Ensuring Network Efficiency – Reducing congestion by filtering unnecessary traffic.

4.3.2 Types of ACLs Implemented

1. Standard ACLs

- Filter based only on source IP addresses.

- Used for basic access restrictions such as blocking devices from reaching certain parts of the network.

2. Extended ACLs

- Filter based on source IP, destination IP, and protocols (TCP, UDP, ICMP, etc.).
- Used for fine-grained security controls, such as allowing only specific services (HTTP, FTP, SSH).

3. Named ACLs

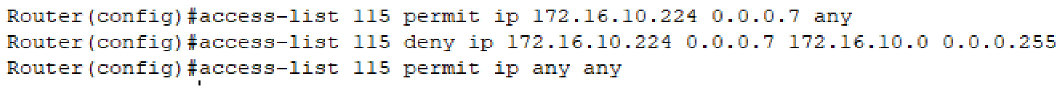
- Instead of numbered ACLs, these are named for better readability and management.
- Used to organize and apply security rules more effectively.

4.3.3 ACL Implementation for Departmental Restrictions

Each department has its own ACL assigned to the respective VLAN interface to ensure controlled communication. Below is the breakdown of implemented ACLs:

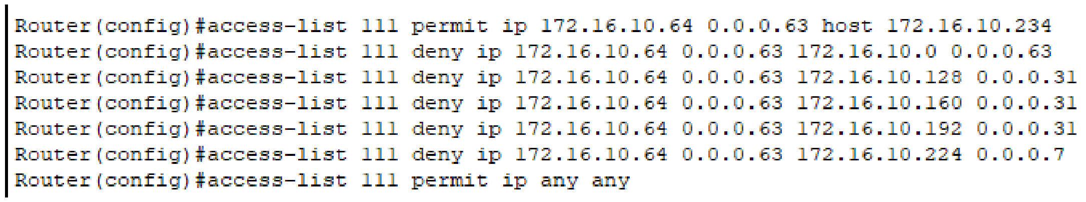
ACL Number	Applied To (Interface/VLAN)	Rules Applied
110	VLAN 10 (Sales)	Permit access to File & Web Server; Deny access to other VLANs.
111	VLAN 20 (Development)	Permit access to Web Server; Deny access to Sales, HR, Finance VLANs.
112	VLAN 30 (IT)	Allow all access (IT requires full network access).
113	VLAN 40 (HR)	Permit access to HR Server; Deny access to Sales, Dev, Finance VLANs.
114	VLAN 50 (Finance)	Permit access to Finance Server; Deny access to Sales, Dev, HR VLANs.
115	GigabitEthernet0/2 (Conference)	Allow DHCP access; Block unauthorized internal traffic.
130	GigabitEthernet0/1 (External)	Block unauthorized external access; Allow permitted outbound traffic.

→ACL Rules



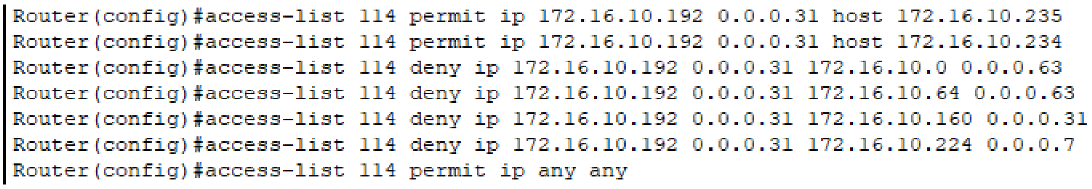
```
Router(config)#access-list 115 permit ip 172.16.10.224 0.0.0.7 any
Router(config)#access-list 115 deny ip 172.16.10.224 0.0.0.7 172.16.10.0 0.0.0.255
Router(config)#access-list 115 permit ip any any
```

Figure: Conference ACL



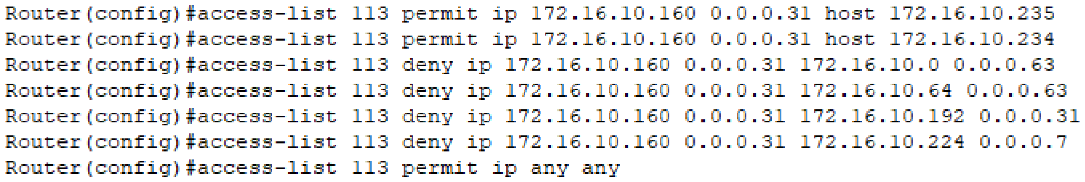
```
Router(config)#access-list 111 permit ip 172.16.10.64 0.0.0.63 host 172.16.10.234
Router(config)#access-list 111 deny ip 172.16.10.64 0.0.0.63 172.16.10.0 0.0.0.63
Router(config)#access-list 111 deny ip 172.16.10.64 0.0.0.63 172.16.10.128 0.0.0.31
Router(config)#access-list 111 deny ip 172.16.10.64 0.0.0.63 172.16.10.160 0.0.0.31
Router(config)#access-list 111 deny ip 172.16.10.64 0.0.0.63 172.16.10.192 0.0.0.31
Router(config)#access-list 111 deny ip 172.16.10.64 0.0.0.63 172.16.10.224 0.0.0.7
Router(config)#access-list 111 permit ip any any
```

Figure: Development ACL



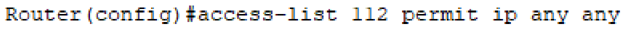
```
Router(config)#access-list 114 permit ip 172.16.10.192 0.0.0.31 host 172.16.10.235
Router(config)#access-list 114 permit ip 172.16.10.192 0.0.0.31 host 172.16.10.234
Router(config)#access-list 114 deny ip 172.16.10.192 0.0.0.31 172.16.10.0 0.0.0.63
Router(config)#access-list 114 deny ip 172.16.10.192 0.0.0.31 172.16.10.64 0.0.0.63
Router(config)#access-list 114 deny ip 172.16.10.192 0.0.0.31 172.16.10.160 0.0.0.31
Router(config)#access-list 114 deny ip 172.16.10.192 0.0.0.31 172.16.10.224 0.0.0.7
Router(config)#access-list 114 permit ip any any
```

Figure: Finance ACL



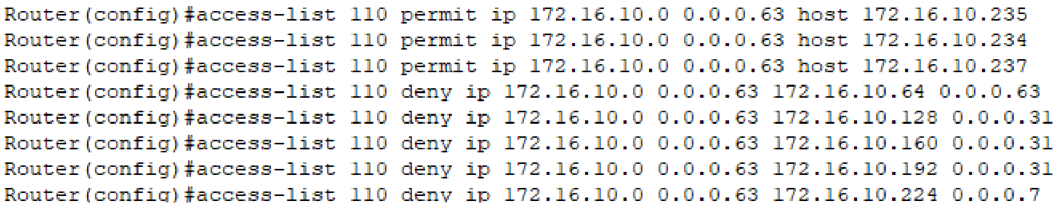
```
Router(config)#access-list 113 permit ip 172.16.10.160 0.0.0.31 host 172.16.10.235
Router(config)#access-list 113 permit ip 172.16.10.160 0.0.0.31 host 172.16.10.234
Router(config)#access-list 113 deny ip 172.16.10.160 0.0.0.31 172.16.10.0 0.0.0.63
Router(config)#access-list 113 deny ip 172.16.10.160 0.0.0.31 172.16.10.64 0.0.0.63
Router(config)#access-list 113 deny ip 172.16.10.160 0.0.0.31 172.16.10.192 0.0.0.31
Router(config)#access-list 113 deny ip 172.16.10.160 0.0.0.31 172.16.10.224 0.0.0.7
Router(config)#access-list 113 permit ip any any
```

Figure: HR ACL



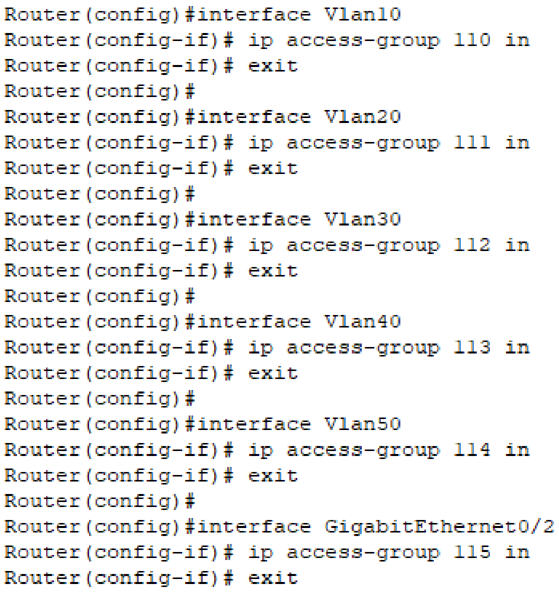
```
Router(config)#access-list 112 permit ip any any
```

Figure: IT ACL



```
Router(config)#access-list 110 permit ip 172.16.10.0 0.0.0.63 host 172.16.10.235
Router(config)#access-list 110 permit ip 172.16.10.0 0.0.0.63 host 172.16.10.234
Router(config)#access-list 110 permit ip 172.16.10.0 0.0.0.63 host 172.16.10.237
Router(config)#access-list 110 deny ip 172.16.10.0 0.0.0.63 172.16.10.64 0.0.0.63
Router(config)#access-list 110 deny ip 172.16.10.0 0.0.0.63 172.16.10.128 0.0.0.31
Router(config)#access-list 110 deny ip 172.16.10.0 0.0.0.63 172.16.10.160 0.0.0.31
Router(config)#access-list 110 deny ip 172.16.10.0 0.0.0.63 172.16.10.192 0.0.0.31
Router(config)#access-list 110 deny ip 172.16.10.0 0.0.0.63 172.16.10.224 0.0.0.7
```

Figure: Sales ACL



```
Router(config)#interface Vlan10
Router(config-if)# ip access-group 110 in
Router(config-if)# exit
Router(config)#
Router(config)#interface Vlan20
Router(config-if)# ip access-group 111 in
Router(config-if)# exit
Router(config)#
Router(config)#interface Vlan30
Router(config-if)# ip access-group 112 in
Router(config-if)# exit
Router(config)#
Router(config)#interface Vlan40
Router(config-if)# ip access-group 113 in
Router(config-if)# exit
Router(config)#
Router(config)#interface Vlan50
Router(config-if)# ip access-group 114 in
Router(config-if)# exit
Router(config)#
Router(config)#interface GigabitEthernet0/2
Router(config-if)# ip access-group 115 in
Router(config-if)# exit
```

Figure: ACL implementation on interfaces

4.3.4 Justification for ACLs Implementation

ACL Feature	Justification
Inter-VLAN ACLs	Restrict departments from unnecessary communication, ensuring data privacy.
Server ACLs	Prevent unauthorized access to File, DHCP, and Web servers.
Inbound/Outbound ACLs	Controls traffic between internal and external networks.
ICMP Blocking	Prevents unauthorized network scanning and reconnaissance attacks.
Explicit Deny Rules	Ensure that only permitted traffic can pass, blocking unknown requests.

Figure: ACLs Justification

4.4 Verification of Security Policies

4.4.1 Purpose of Security Policy Verification

Security policies must be verified and tested to ensure they function as intended. The purpose of verification includes:

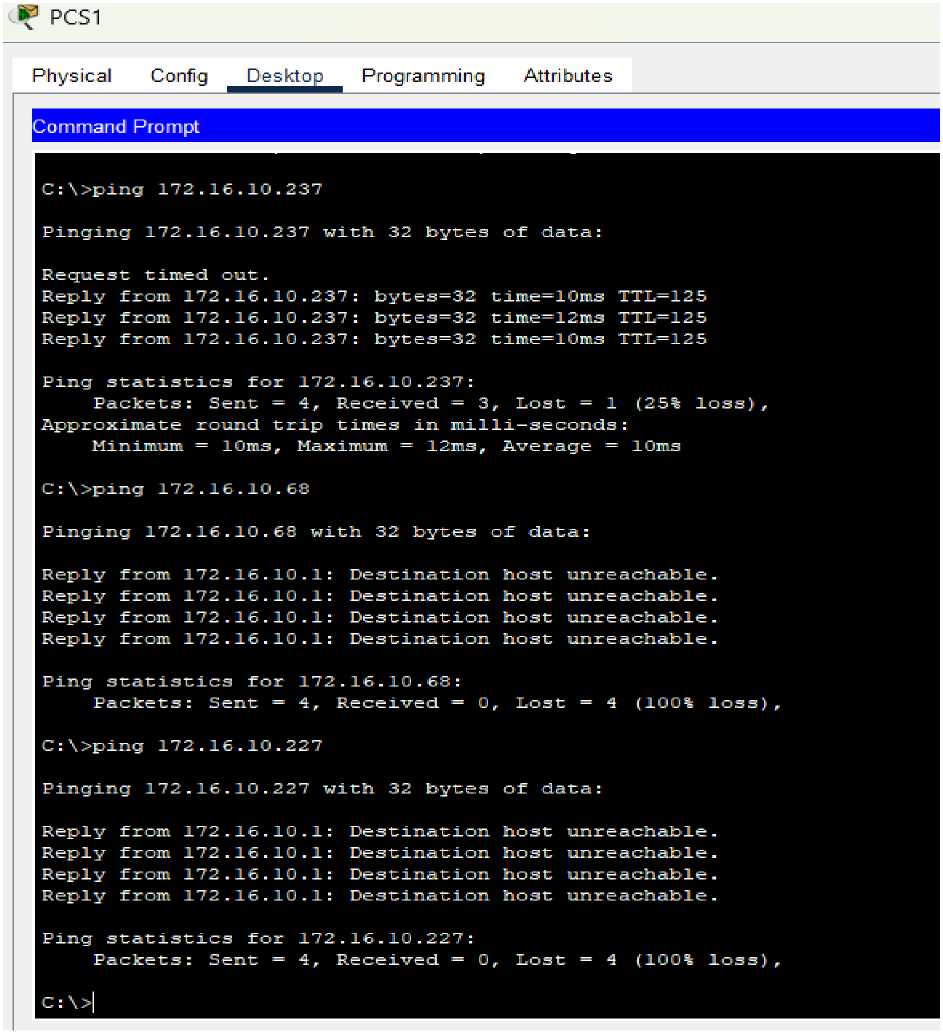
1. Confirming that ACLs are properly applied to block unauthorized access.
2. Validating firewall rules to ensure expected traffic flow is maintained.
3. Testing VLAN segmentation to confirm that inter-VLAN restrictions work correctly.
4. Monitoring network logs to detect anomalies and potential security violations.
5. Ensuring compliance with industry security standards.

4.4.2 Security Policy Verification Methods

1. Testing ACL and ZPF Rules Using Ping:

Each ACL and ZPF is tested using ping command to confirm blocked and allowed traffic.

In the below figure Sales PC when trying to ping other department PCs gets an unreachable message but can ping Email Server which justifies our ACL rules implementation.



```
C:\>ping 172.16.10.237

Pinging 172.16.10.237 with 32 bytes of data:

Request timed out.
Reply from 172.16.10.237: bytes=32 time=10ms TTL=125
Reply from 172.16.10.237: bytes=32 time=12ms TTL=125
Reply from 172.16.10.237: bytes=32 time=10ms TTL=125

Ping statistics for 172.16.10.237:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 10ms

C:\>ping 172.16.10.68

Pinging 172.16.10.68 with 32 bytes of data:

Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.

Ping statistics for 172.16.10.68:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.16.10.227

Pinging 172.16.10.227 with 32 bytes of data:

Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.
Reply from 172.16.10.1: Destination host unreachable.

Ping statistics for 172.16.10.227:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure: Sales PC Ping test

5. Advanced Security Configuration

5.1 Remote Branch Setup

5.1.1 Purpose of Remote Branch Setup

The remote branch setup is designed to connect a geographically separate office to the main network at Tech Zolutions Inc. securely and efficiently. The Remote Branch Router establishes connectivity using IPsec Site-to-Site VPN, ensuring encrypted communication over the public internet while providing seamless access to internal services such as file sharing, email, and web applications.

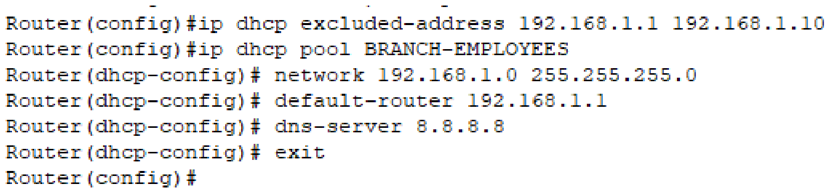
5.1.2 Objectives of Remote Branch Setup

- Secure Connectivity - Establish a secure tunnel between the remote office and the main network.
- Resource Sharing - Ensure remote users can access internal services (Web Server, File Server, Email).
- Scalability - Provide a setup that allows for additional branches in the future.
- Efficient Routing - Use OSPF for dynamic routing between locations.
- DHCP Configuration - Assign IP addresses dynamically to branch employees.

5.1.3 Configuration of Remote Branch Router

The Remote Branch Router is configured to manage local clients while maintaining secure communication with the main office. The 192.168.1.0/24 subnet is used as the base network.

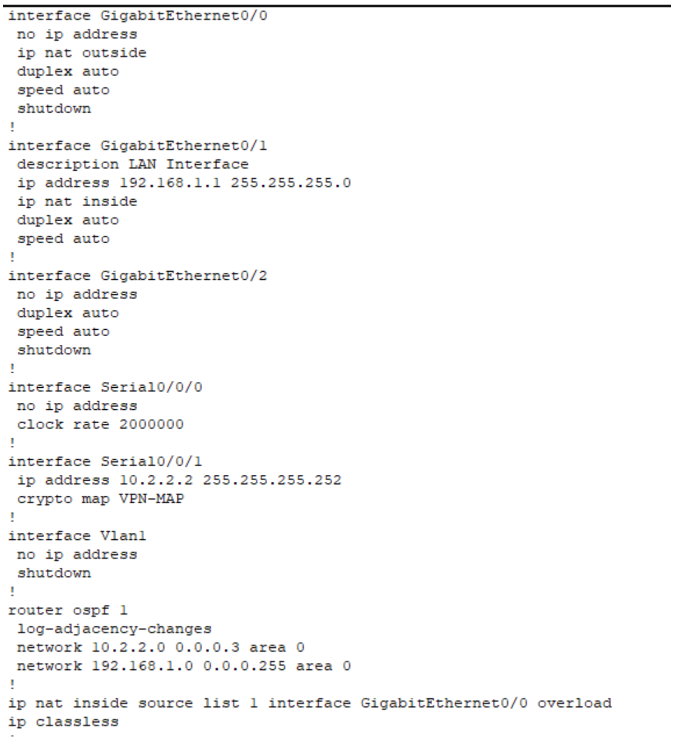
Step 1: Configuring DHCP on the Remote Branch Router



```
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
Router(config)#ip dhcp pool BRANCH-EMPLOYEES
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# exit
Router(config)#
```

Figure: DHCP Configuration

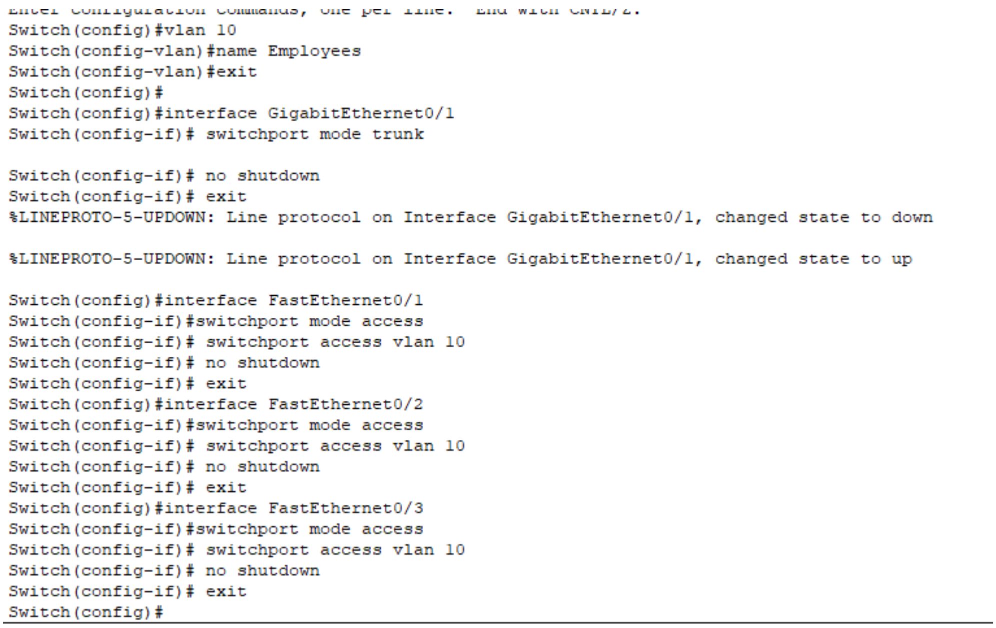
Step 2: Configuring LAN and WAN Interfaces and Configure OSPF for Dynamic Routing



```
interface GigabitEthernet0/0
 no ip address
 ip nat outside
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 description LAN Interface
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 crypto map VPN-MAP
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip classless
```

Figure: Router Configuration and OSPF

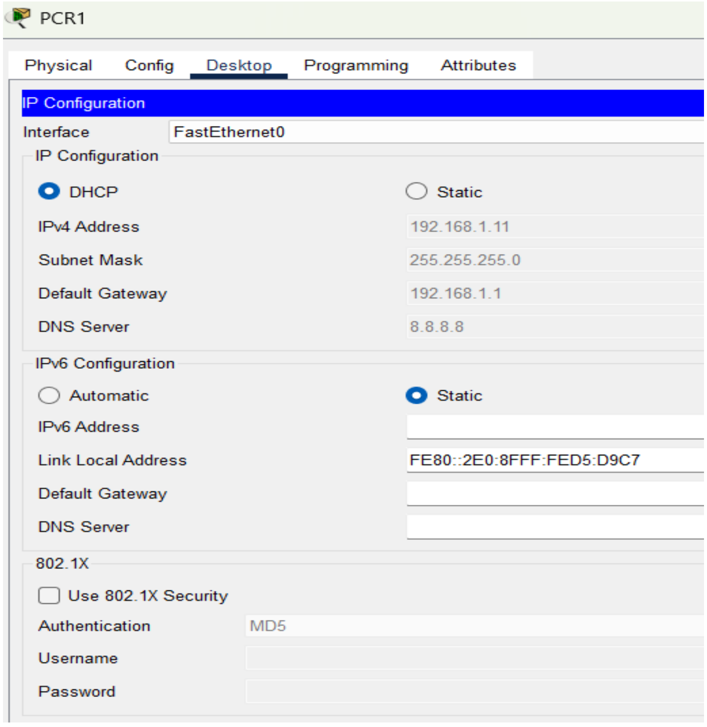
Step 4: Switch setup



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Employees
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk

Switch(config-if)# no shutdown
Switch(config-if)# exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)#
```

Figure: Remote Branch Switch Configuration

Step 5: Configure Dynamic DHCP on Endpoint Devices



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.1.11

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address

Link Local Address FE80::2E0:8FFF:FED5:D9C7

Default Gateway

DNS Server

802.1X

□ Use 802.1X Security

Authentication MD5

Username

Password

Figure: Endpoint Device Configuration

5.2 Site-to-Site VPN Implementation (IPsec)

5.2.1 Purpose of Site-to-Site VPN Implementation

The Site-to-Site VPN is implemented to establish a secure encrypted tunnel between the remote branch and the main office. This allows branch employees to access internal resources as if they were physically present at the headquarters, while ensuring security over an untrusted internet connection.

5.2.2 Objectives of Site-to-Site VPN Implementation

- Encrypt traffic between branch and main office using IPsec.
- Ensure secure access to internal resources (File Server, Email, Web).
- Prevent unauthorized interception of data over public internet.
- Authenticate and validate devices before allowing access.

5.2.3 IPsec VPN Configuration

The VPN configuration is applied on both the Main Router and Remote Branch Router.

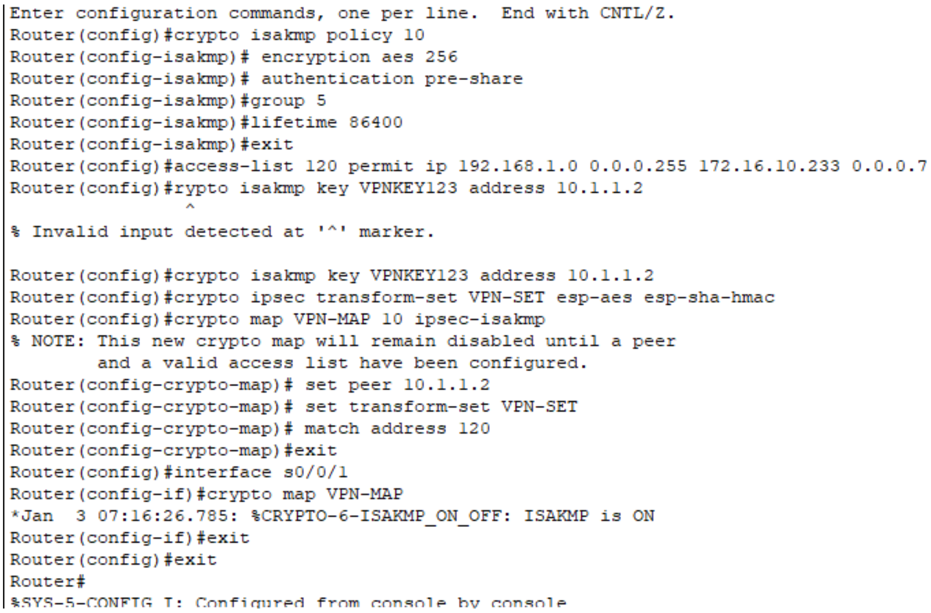
Step 1: Define IPsec ISAKMP Policy (Main & Remote Routers)

Step 2: Configure Pre-Shared Key for Authentication

Step 3: Define IPsec Transform Set for Encryption

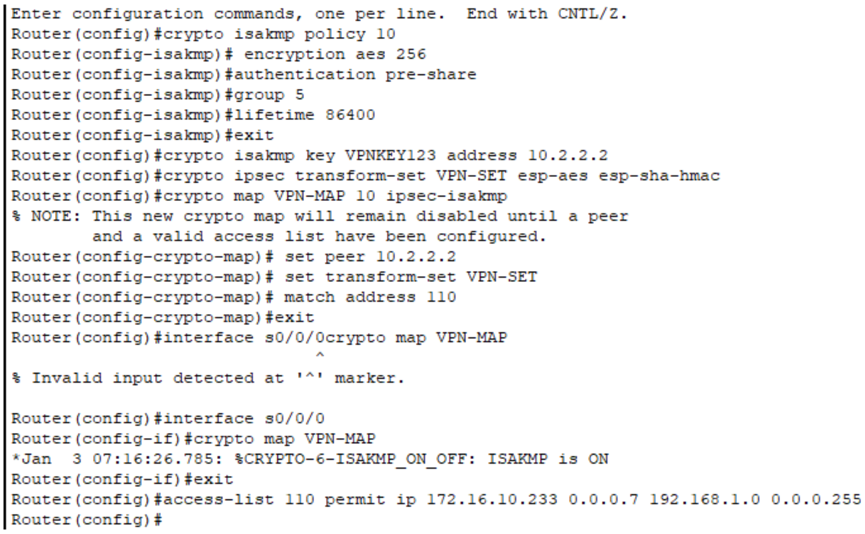
Step 4: Create Crypto Map and Apply It to Interfaces

Step 5: Apply ACL to Define Interesting Traffic



```
Enter configuration commands, one per line.  End with CNTL/Z.
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)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#access-list 120 permit ip 192.168.1.0 0.0.0.255 172.16.10.233 0.0.0.7
Router(config)#rypto isakmp key VPNKEY123 address 10.1.1.2
                ^
% Invalid input detected at '^' marker.

Router(config)#crypto isakmp key VPNKEY123 address 10.1.1.2
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)# set peer 10.1.1.2
Router(config-crypto-map)# set transform-set VPN-SET
Router(config-crypto-map)# match address 120
Router(config-crypto-map)#exit
Router(config)#interface s0/0/1
Router(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure: IPsec VPN Configuration on Remote Router



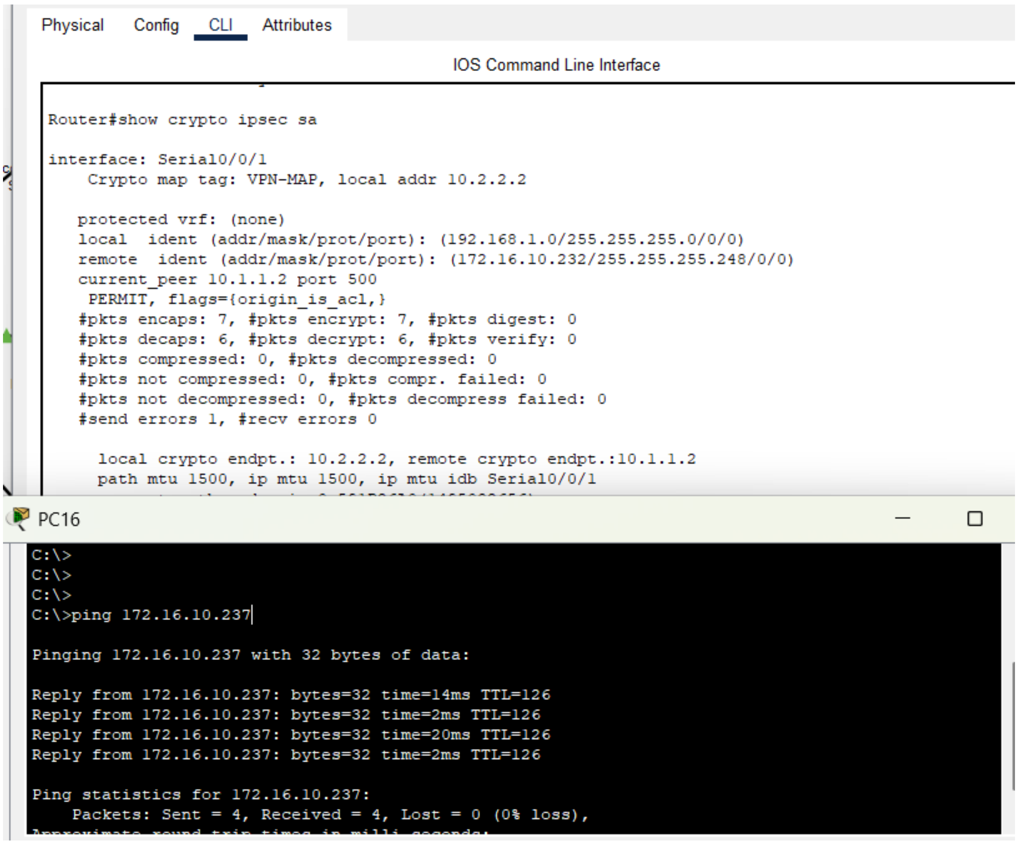
```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)# encryption aes 256
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#crypto isakmp key VPNKEY123 address 10.2.2.2
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)# set peer 10.2.2.2
Router(config-crypto-map)# set transform-set VPN-SET
Router(config-crypto-map)# match address 110
Router(config-crypto-map)#exit
Router(config)#interface s0/0/0crypto map VPN-MAP
                               ^
% Invalid input detected at '^' marker.

Router(config)#interface s0/0/0
Router(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#access-list 110 permit ip 172.16.10.233 0.0.0.7 192.168.1.0 0.0.0.255
Router(config)#
```

Figure: IPsec VPN Configuration on External Router

5.2.4 Verifying Site-to-Site VPN Connection

After configuration, we verify the VPN status to ensure secure communication.

When pinging Email server from Remote PC we can se encrypted packets using command - “show crypto ipsec sa”



```
Router#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: VPN-MAP, local addr 10.2.2.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.10.232/255.255.255.248/0/0)
   current_peer 10.1.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #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.: 10.2.2.2, remote crypto endpt.:10.1.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
```

```
C:\>
C:\>
C:\>
C:\>ping 172.16.10.237

Pinging 172.16.10.237 with 32 bytes of data:

Reply from 172.16.10.237: bytes=32 time=14ms TTL=126
Reply from 172.16.10.237: bytes=32 time=2ms TTL=126
Reply from 172.16.10.237: bytes=32 time=20ms TTL=126
Reply from 172.16.10.237: bytes=32 time=2ms TTL=126

Ping statistics for 172.16.10.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Figure: VPN connectivity results

5.3 AAA Server Configuration for Authentication and Authorization

5.3.1 Purpose of AAA Server Implementation

Authentication, Authorization, and Accounting (AAA) is a security framework used to manage access control, verify user identities, and log administrative activities on network devices. The AAA implementation using TACACS+ ensures that only authorized personnel can access network resources, and their activities are logged for security auditing.

The primary objectives of implementing AAA with a TACACS+ server in Tech Zolutions Inc. are:

1. Secure Remote Authentication - Prevent unauthorized access to routers and switches.
2. Centralized User Management - Users authenticate against a centralized TACACS+ server instead of local device credentials.
3. Granular Authorization Controls - Assign different privilege levels to users based on their roles.
4. Logging and Accountability - Maintain an audit trail of administrative activities for security compliance.

5. Enhanced Network Security - Reduce the risk of brute-force attacks and unauthorized access.

5.3.2 AAA Server Configuration Overview

Network Components Involved in AAA Authentication

- TACACS+ Server – Located at IP 172.16.10.238, handling authentication requests.
- Main Router – Configured to forward authentication requests to the TACACS+ server.
- Remote Branch Router – Also integrated with the TACACS+ server for remote authentication.

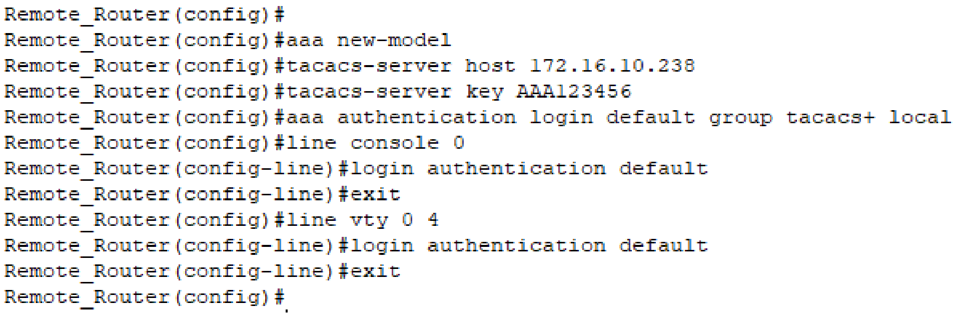
5.3.3 AAA Configuration on Network Devices

Step 1: Enable AAA on Main and Remote Routers

Step 2: Define TACACS+ Server Details

Step 3: Configure Authentication Method

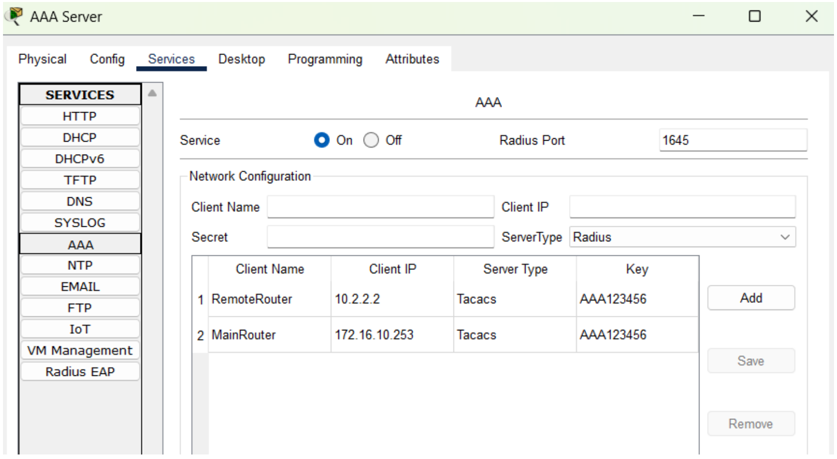
Step 4: Apply AAA Authentication to Console and VTY Lines



```
Remote_Router(config)#
Remote_Router(config)#aaa new-model
Remote_Router(config)#tacacs-server host 172.16.10.238
Remote_Router(config)#tacacs-server key AAA123456
Remote_Router(config)#aaa authentication login default group tacacs+ local
Remote_Router(config)#line console 0
Remote_Router(config-line)#login authentication default
Remote_Router(config-line)#exit
Remote_Router(config)#line vty 0 4
Remote_Router(config-line)#login authentication default
Remote_Router(config-line)#exit
Remote_Router(config)#
```

Figure: AAA Configuration on Remote Router

Same Steps have been followed for Main Router.



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	RemoteRouter	10.2.2.2	Tacacs	AAA123456
2	MainRouter	172.16.10.253	Tacacs	AAA123456

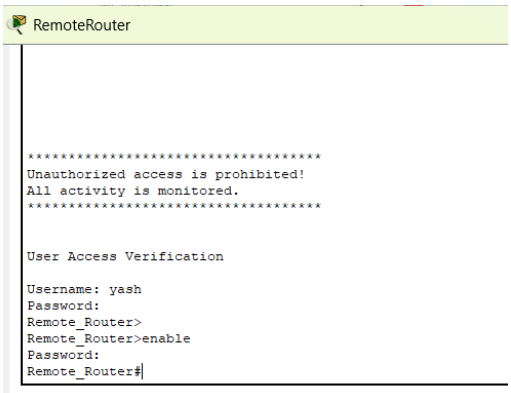
Figure: AAA server Configuration

5.3.4 Verification of AAA Authentication

After configuring AAA on the routers, administrators can verify that the TACACS+ authentication is working.

Method 1: Testing Authentication via Console Login

When a user tries to log in to the Remote Router, they are prompted for a username and password managed by the TACACS+ server. Same works for Main Router.



```
************************************
Unauthorized access is prohibited!
All activity is monitored.
************************************


User Access Verification

Username: yash
Password:
Remote_Router>
Remote_Router>enable
Password:
Remote_Router#
```

Figure: AAA test

Successful authentication confirms that the router is verifying credentials via the TACACS+ server.

5.3.5 Justification for use of TACACS+ Server

Implementing a TACACS+ server in Tech Zolutions Inc. ensures:

- Centralized authentication for all network devices, improving security and efficiency.
- Role-based access control (RBAC) to enforce least-privilege policies.
- End-to-end encryption of authentication traffic, preventing credential leaks.
- Comprehensive logging and auditing, ensuring compliance with security policies.
- Granular command authorization, allowing fine-tuned control over administrator privileges.

6. Conclusion and Recommendations

6.1 Summary of Findings

The implementation of Tech Zolutions Inc.'s network infrastructure has been successfully designed and deployed, ensuring a secure, scalable, and high-performance enterprise network. The network architecture integrates efficient subnetting, VLANs, OSPF routing, security configurations, remote branch connectivity, and authentication mechanisms to meet the organization's operational and security requirements.

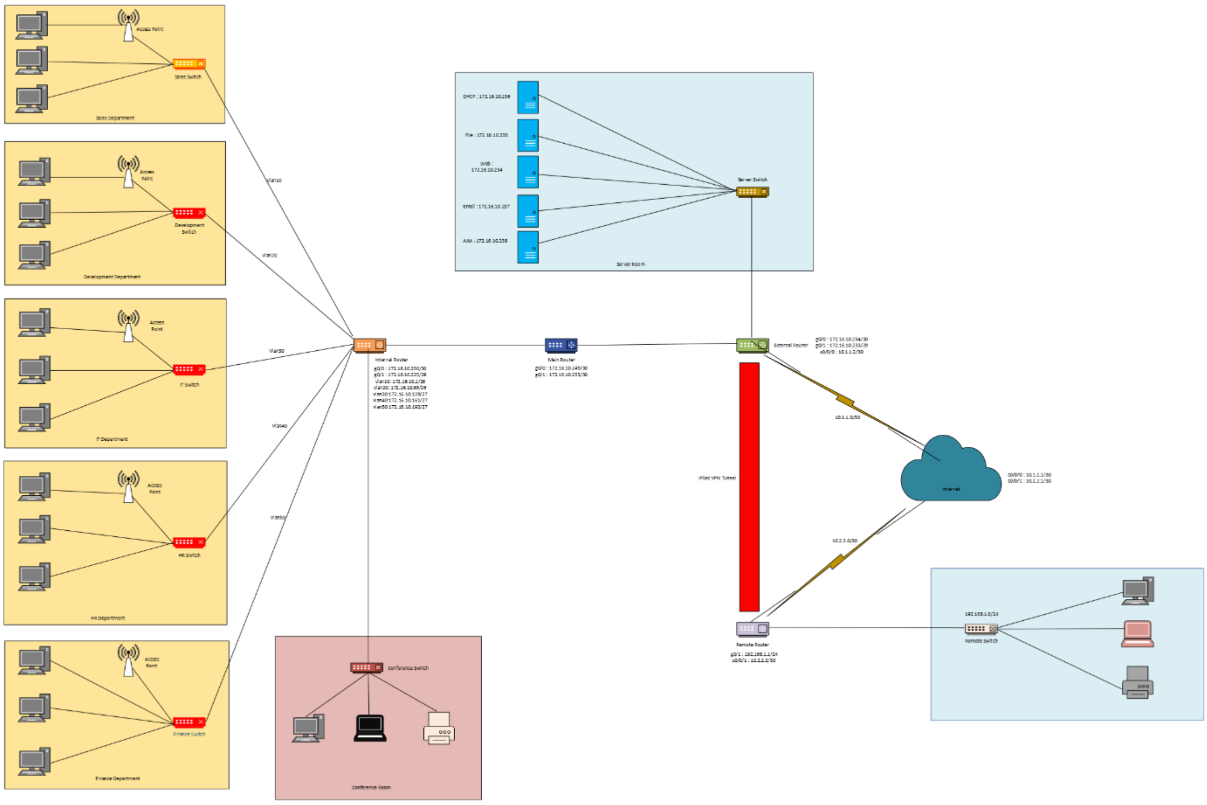


Figure: Final Network Topology

6.1.1 Key Achievements and Findings

Component	Findings and Achievements
Network Segmentation	Implemented VLANs to logically separate departments, reducing broadcast traffic and improving security by restricting inter-departmental communication where necessary.
IP Addressing and Subnetting	Designed an optimized subnetting scheme based on departmental needs, ensuring efficient IP allocation and reducing the risk of IP conflicts.
Routing and Connectivity	Configured OSPF (Open Shortest Path First) as the dynamic routing protocol to provide fast convergence, efficient path selection, and redundancy across network segments.

Security Policies	Applied ACLs (Access Control Lists), Firewall Rules, and AAA authentication to restrict access to critical resources and enforce security policies.
Wireless Network Setup	Deployed secure departmental Wi-Fi networks with appropriate authentication mechanisms to ensure secure access to internal resources.
Remote Branch Connectivity	Established a secure Site-to-Site VPN using IPsec encryption to connect the remote office to the main network, ensuring data confidentiality and integrity over the public internet.
AAA Authentication and Authorization	Implemented TACACS+ authentication for administrative access, providing centralized user authentication, authorization, and accounting to track and control network access.
Threat Mitigation and Security Enhancements	Applied firewall policies, access control rules, and network monitoring configurations to prevent unauthorized access, data breaches, and security threats.

Figure: Key Achievements

The implemented network successfully meets the organization's functional and security requirements, ensuring reliable communication, efficient resource allocation, and robust access control.

6.2 Recommendations for Future Enhancements

While the current network infrastructure provides a strong foundation for security, efficiency, and scalability, certain enhancements can be implemented in the future to further strengthen security, improve performance, and support business growth.

6.2.1 Security Enhancements

1. Implement Multi-Factor Authentication (MFA) for Network Administrators:

- While TACACS+ authentication secures login access, adding MFA (such as OTP-based verification or biometric authentication) would provide an extra security layer.
- This would mitigate risks associated with stolen credentials and reduce brute-force attacks.

2. Deploy Network Access Control (NAC) for Endpoint Security

- Network Access Control (NAC) ensures that only authorized and compliant devices can connect to the network.
- Prevents unauthorized devices (e.g., personal laptops or rogue IoT devices) from accessing internal resources.

3. Upgrade to Next-Generation Firewalls (NGFWs)

- Traditional firewalls operate at Layer 3 (IP-based filtering), whereas NGFWs provide deep packet inspection (DPI), intrusion prevention, and application-layer filtering.
- Enhances detection and prevention of advanced cyber threats such as malware, ransomware, and unauthorized application usage.

4. Strengthen VPN Security with Redundant Tunnels

- While IPsec VPN ensures secure communication, a single VPN tunnel introduces a single point of failure.
- Redundant tunnels provide high availability (HA) and automatic failover in case of primary tunnel failure.

5. Conduct Periodic Penetration Testing and Security Audits

- Even with strong security measures, new vulnerabilities can emerge over time.
- Penetration testing helps identify weak spots in ACLs, firewall policies, and access configurations.

6.2.2 Performance and Scalability Enhancements

1. Transition to IPv6 for Future Network Growth

- IPv4 address exhaustion is a growing concern, and IPv6 provides a larger address space.
- IPv6 offers enhanced security features, simplified routing, and improved multicast support.

2. Deploy Software-Defined Networking (SDN) for Network Automation

- SDN enables centralized control of network resources, improving scalability, performance, and automation.
- Reduces manual configuration errors by allowing administrators to automate VLAN, routing, and security policy changes.

6.2.3 Monitoring and Compliance Enhancements

1. Implement Security Information and Event Management (SIEM) for Threat Detection

- SIEM solutions centralize logs, analyze security incidents, and provide real-time alerts.
- Helps in detecting anomalous behavior, brute-force attacks, and insider threats.

2. Enable Role-Based Access Control (RBAC) for Network Management

- Not all IT personnel require full administrative privileges.
- RBAC ensures that users only have the access necessary for their job functions.

6.2.4 Conclusion

The Tech Zolutions Inc. network implementation has successfully met the objectives of secure, scalable, and efficient connectivity across departments and remote branches. By integrating advanced security controls, AAA authentication, firewall policies, and VLAN segmentation, the network provides robust security while ensuring optimal performance.

By implementing the recommended future enhancements, the organization can:

- Future-proof its infrastructure against evolving security threats.
- Enhance operational efficiency through automation and network analytics.
- Ensure compliance with security best practices and regulatory frameworks.
- Improve fault tolerance and business continuity with redundant VPN tunnels.

This will enable Tech Zolutions Inc. to continue growing its IT capabilities while maintaining a highly secure and resilient network infrastructure.

7. References

- Stallings, W. (2020) *Network Security Essentials: Applications and Standards.* 6th edn. Pearson.
- Kurose, J. and Ross, K. (2021) *Computer Networking: A Top-Down Approach.* 8th edn. Pearson.
- Cisco (2023) *Cisco IOS Security Configuration Guide.* Available at: https://www.cisco.com/c/en/us/td/docs/ios/security/configuration
- IETF (2023) *RFC 2401 – Security Architecture for IPsec.* Internet Engineering Task Force. Available at: https://tools.ietf.org/html/rfc2401
- NIST (2021) *Security Recommendations for Enterprise Networks.* National Institute of Standards and Technology.
- Cisco Networking Academy (2023) *Routing and Switching Essentials.* Available at: https://www.netacad.com
- Juniper Networks (2023) *OSPF and BGP Configuration Guide.* Available at: https://www.juniper.net/documentation
- SANS Institute (2024) *Best Practices for Network Security and Access Control.* Available at: https://www.sans.org/white-papers
- TechTarget (2024) *Firewall Policies and Access Control Lists Best Practices.* Available at: https://www.techtarget.com