Module Leader

Muhammad Ali

NEtwork Routing report for fintec inc.

Module: MOD003262 TRI2 F01CAM  
[Word Count:2800]



**STUDENT ID: 2317058**

Table of Contents

[1. Introduction 2](#_Toc191484042)

[1.1 Purpose of the Report 2](#_Toc191484043)

[1.2 Background and Business Needs 2](#_Toc191484044)

[1.3 Objectives 2](#_Toc191484045)

[2. Network Design Overview 3](#_Toc191484046)

[2.1 Existing Network Structure 3](#_Toc191484047)

[2.2 Proposed Network Topology 3](#_Toc191484048)

[2.3 VLAN Implementation 5](#_Toc191484049)

[3. Routing Strategy 5](#_Toc191484050)

[3.1 Routing Protocol Selection 5](#_Toc191484051)

[3.2 IP Addressing Scheme 11](#_Toc191484052)

[4. Switching & DHCP Implementation 13](#_Toc191484053)

[4.1 VLAN Configuration 13](#_Toc191484054)

[4.2 DHCP Implementation 16](#_Toc191484055)

[5. Network Security Implementation 25](#_Toc191484056)

[5.1 Access Control & Security Policies 25](#_Toc191484057)

[5.2 Device Hardening Measures 30](#_Toc191484058)

[6. Testing & Validation 37](#_Toc191484059)

[6.1 Connectivity Testing 37](#_Toc191484060)

[6.2 Security Testing 40](#_Toc191484061)

[7. Conclusion & Recommendations 40](#_Toc191484062)

[8. References 41](#_Toc191484063)

# 1. Introduction

## 1.1 Purpose of the Report

## FinTec Inc. Will gain from a complete community design notion focused on improving efficiency, safety, and scalability. The solution addresses routing demanding situations, records segmentation, and steady connectivity even as making sure a resilient infrastructure aligned with industrial corporation targets. Advanced technology which includes SDN, VLAN segmentation, and subsequent-era firewalls optimize traffic drift and decrease latency. Redundant links and sturdy failover protocols improve availability and mitigate downtime dangers. An incredible risk evaluation, rate assessment, and phased implementation plan make sure managed deployment and future boom. The idea moreover includes monitoring tools and ordinary audits to hold compliance and address evolving threats, ensuring non-forestall operational excellence.

## 1.2 Background and Business Needs

FinTec Inc. operates across four sites London, Leeds, Liverpool, and Leicester with plans to expand its operations and strengthen its network infrastructure. The current network setup is outdated, lacks scalability, and faces security vulnerabilities that could impact operational continuity. Therefore, a robust networking solution is required to:

* Improve inter-site connectivity.
* Implement efficient data routing.
* Enhance network security and access control.
* Optimize resource allocation using VLAN segmentation and dynamic IP addressing.

## 1.3 Objectives

This project focuses on designing an optimal network topology that:

1. Implement **VLAN segmentation** to partition the network into distinct broadcast domain names. This shape optimizes records glide via decreasing broadcast visitors, improving safety via isolation of touchy segments, and improving overall performance with the aid of minimizing congestion on character community segments.
2. Utilize **OSPF dynamic routing protocols** to decide the first-class records paths robotically. This enhances community efficiency with the resource of fixing to topology changes in real time, provides fast convergence at some point of hyperlink failures, and improves fault tolerance by way of way of dynamically rerouting site visitors to hold connectivity.
3. **Configure DHCP** for computerized, dynamic IP address undertaking. This minimizes manual configuration errors, quickens network deployment, and ensures inexperienced allocation of IP addresses all through a developing infrastructure.
4. **Establish ACL** get proper of access to manipulate rules to secure facts transmission throughout websites. These encompass authentication protocols and firewalls that restriction unauthorized get right of entry to and screen community traffic.
5. Design the community with **Redundancy and Fault Tolerance** to ensure uninterrupted provider. This making plan mitigates the danger of downtime by means of automatically switching to backup sources all through disasters.

# 2. Network Design Overview

## 2.1 Existing Network Structure

FinTec Inc. currently has four locations: London, Leeds, Liverpool, and Leicester. The existing network is limited in scalability, lacks efficient security policies, and requires optimization to meet the growing needs of the organization.

* **Limited network capacity**: The network does not support a large number of devices, creating bottlenecks.
* **Lack of redundancy**: Service disruptions occur due to the absence of backup routes.
* **Poor security implementation**: The network is vulnerable to unauthorized access and data breaches.
* **Inefficient routing**: Static routing methods contribute to slow data transmission.

## 2.2 Proposed Network Topology

The proposed network topology addresses these challenges by implementing the following features:

* **A four-site interconnected architecture**: Each site is hooked up thru excessive-pace fibre links, ensuring minimal latency and high throughput. This setup helps actual-time records synchronization, faraway useful resource sharing, and coordinated catastrophe recuperation across all places.
* **Centralized internet gateway at the London site**: The London net page serves due to the fact the primary access point for all internet traffic. This centralization allows for uniform security rules, streamlined tracking, and efficient bandwidth control on the equal time as supplying a managed get entry to and exit point for out of doors conversation.
* **Redundant links between sites**: Multiple physical and logical connections are hooked up among sites to prevent service disruption. These redundant paths make certain that if one hyperlink fails, network is routinely rerouted, retaining uninterrupted network overall performance and excessive availability.
* **Layer 3 switching for VLAN segmentation**: Each site employs Layer three switches to control inter-VLAN routing effectively. This approach no longer simplest segments the network to lessen broadcast domains however additionally enhances protection and improves traffic control through directing packets based on IP routing protocols.
* **Virtual Private Network (VPN) for secure site-to-site communication**: A robust VPN answer encrypts facts transmitted among branch places of work, making sure that sensitive info is securely exchanged over public networks. The VPN configuration includes multi-component authentication and superior encryption requirements to guard in opposition to cyber threats.
* **Access Control Lists (ACLs) to restrict internet access for non-London sites**: ACLs are configured on routers at each site to implement coverage regulations, allowing best authorized traffic. With this setup, non-London sites are avoided from direct internet connection.
* **Network Address Translation (NAT) and Firewall Implementation**: NAT is deployed to mask inner IP addresses, improving safety via preventing direct outside get admission to the internal community. Combined with present day firewall rules, this configuration protects towards unauthorized intrusions and complies with security regulations at the same time as monitoring and filtering

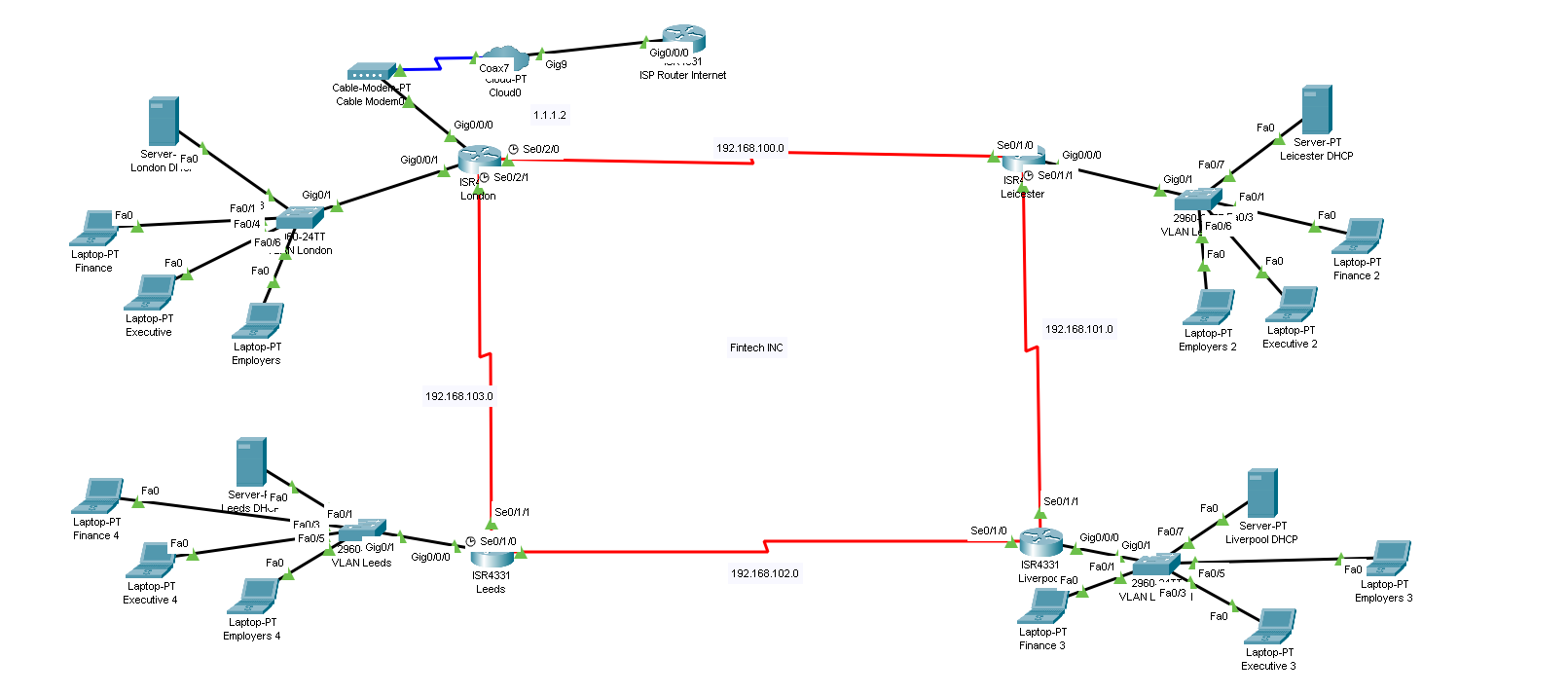
**Network Topology Diagram:**

Figure 1.0 (Topology)

So this is the proposed Topology Diagram (figure a) for the network. Here we are using an example IP 1.1.1.2 for representing internet or ISP router. The configuration of the routers and the network is same as mentioned above. Four sites each with a switch in VLAN configuration and VLSM for creating subnets to avoid wastage of IP’s.

## 

## 2.3 VLAN Implementation

Each site will have three VLANs to segment network traffic effectively:

* **VLAN 30 - Finance:** Restricted access to financial personnel.
* **VLAN 40 - Executive:** Limited to executive management.
* **VLAN 50 - Employers:** General workforce access.

Inter-VLAN routing will be configured using Layer 3 switches, ensuring secure and efficient data exchange among VLANs.

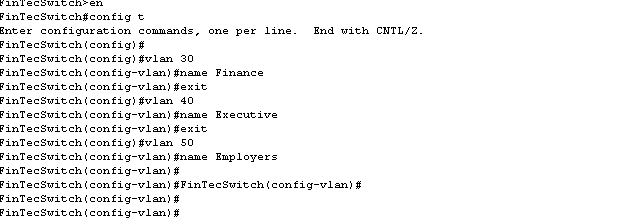


Figure 2.1 (VLAN)

In above Diagram, we are dividing the switch into 3 VLANS and naming them as mentioned Finance, Executive and Employers.

# 3. Routing Strategy

## 3.1 Routing Protocol Selection

To ensure efficient and resilient routing, the following protocols will be implemented:

* **OSPF (Open Shortest Path First):** Chosen for its scalability, quick convergence, and hierarchical design.

Open Shortest Path First (OSPF) is a routing method that helps networks decide the best way to send information from one device to another. Think of OSPF as a smart GPS for network traffic. Just as a GPS finds the quickest route by considering current road conditions, OSPF continually checks different paths within a network to select the most efficient one for data to travel.  
  
One of the key advantages of OSPF is its ability to confirm quick whilst the network adjustments. For instance, if a connection fails or turns into congested, OSPF automatically recalculates the routes, ensuring that the information still finds its manner to the vacation spot without tons delay. This dynamic nature of OSPF makes the community greater resilient and enables save you downtime.  
  
OSPF divides a big community into smaller, more possible sections, making it less difficult to organize site visitors. This department helps hold records flowing smoothly and decreases the possibilities of any one part of the network becoming overloaded. By using OSPF, businesses can preserve dependable, fast conversation across unique elements in their network while not having constant manual changes.

* **Static Routing:** Configured as a backup in case OSPF fails.

**OSPF Configuration Example:**

**Routing config & ARP-Table London**

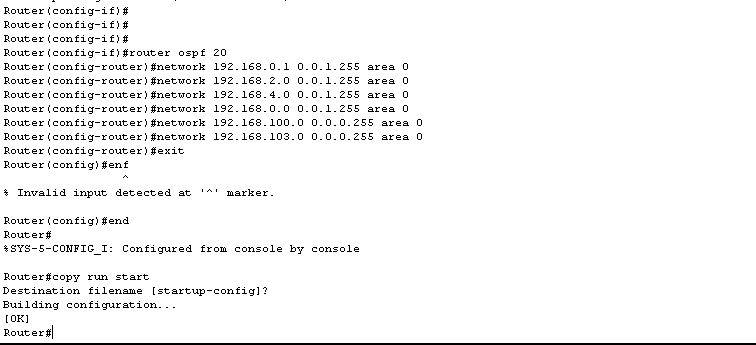


Figure 3.1 (routing OSPF london)

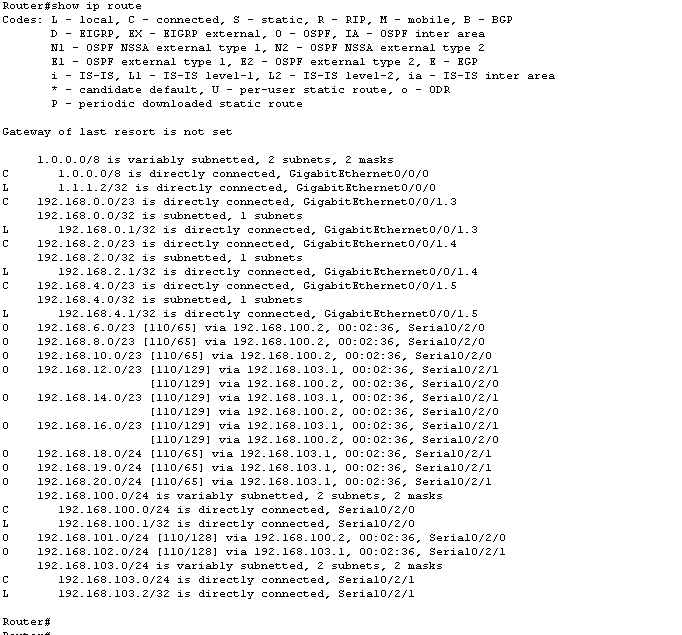


Figure 3.2 (routing table London)

**Routing config & ARP-Table Leicester**

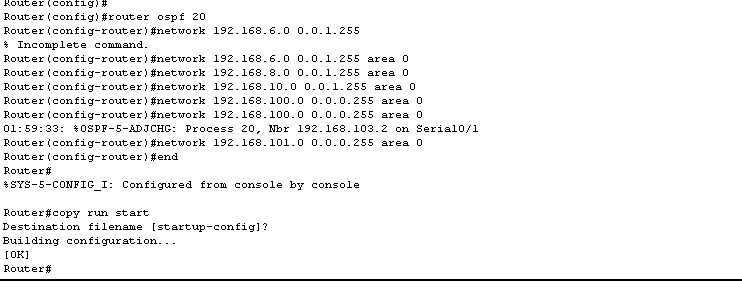


Figure 3.3 (routing OSPF Leicester)

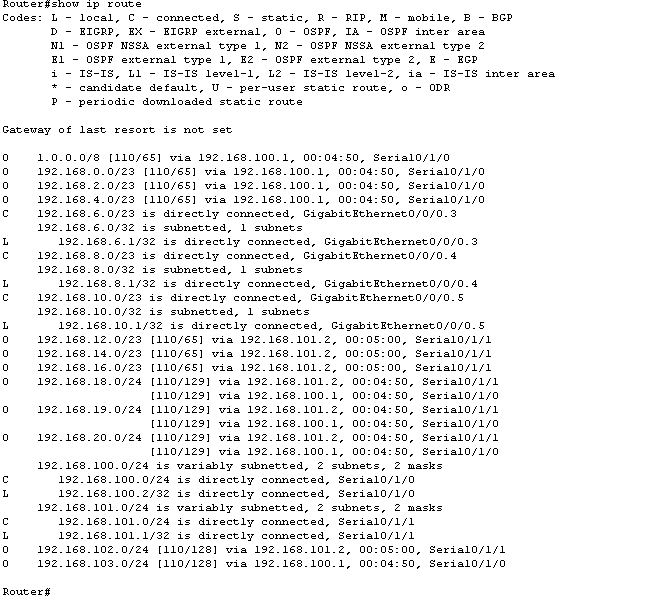


Figure 3.4 (routing table Leicester)

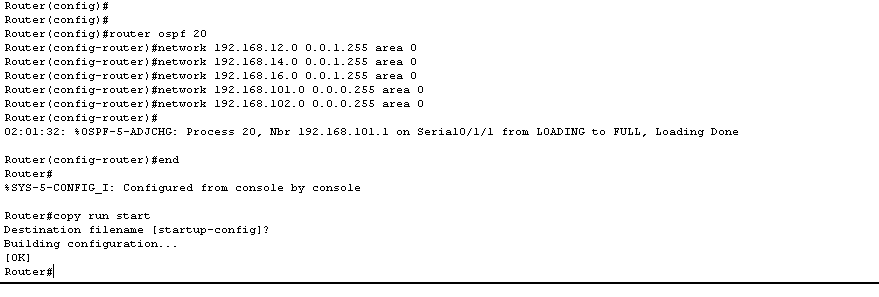
**Routing config & ARP-Table Liverpool**

Figure 3.5 (routing OSPF Liverpool)

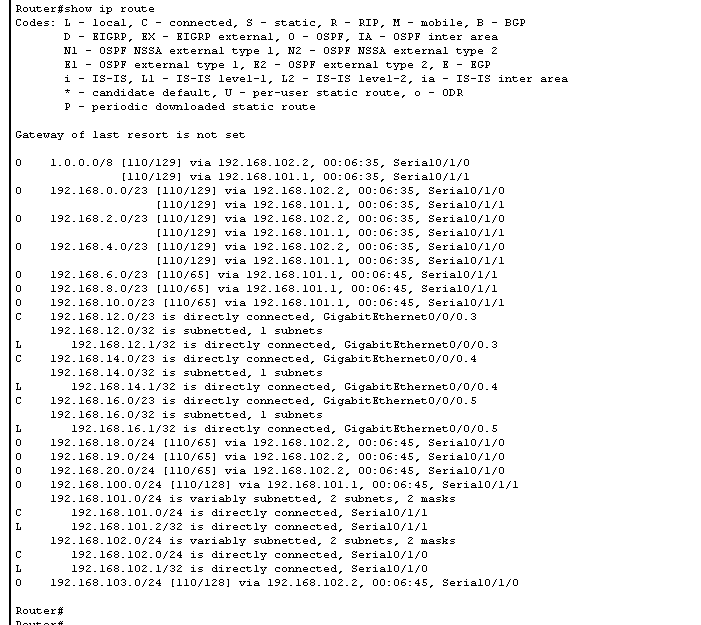
****

Figure 3.6 (routing table Liverpool)

**Routing config & ARP-Table Leeds**

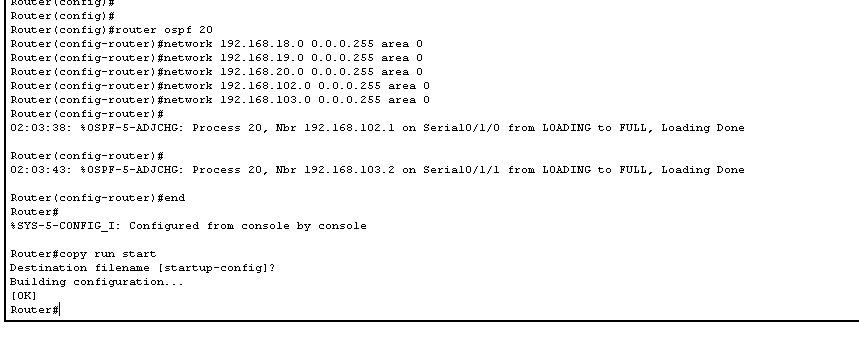


Figure 3.7 (routing OSPF Leeds)

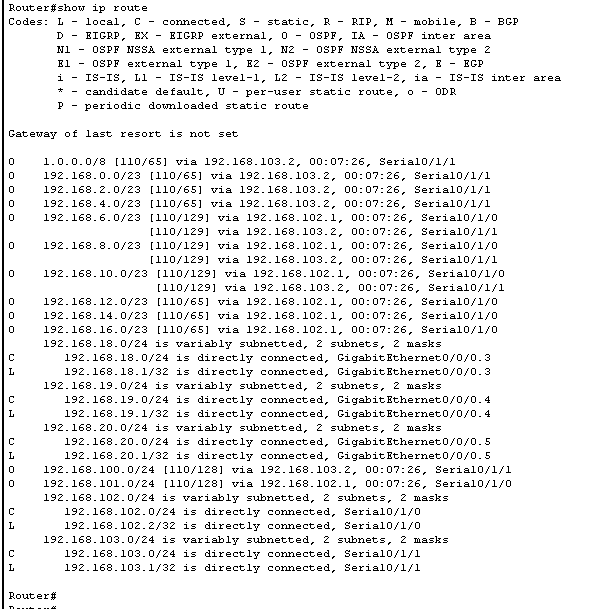


Figure 3.8 (routing table Leeds)

We are using a Dynamic Routing protocol like OSPF (Figure 3.1-3.8) to handle our routing efficiently, this will insure fast routing speeds and a reliable internet connection throughout all four branches.

## 

## 3.2 IP Addressing Scheme

A **Variable Length Subnet Masking (VLSM)** strategy is used for optimal IP allocation. If we consider 192.168.0.0\16 as a starting IP network, then we can implement the subnets for all four branches. The reason is because a class A IP has 256 IPs and we need 1500+1200+900+500 = 4100 IP addresses

**Example:**

**London-1500 hosts**

1500/3 = 500 per VLAN then

Log2(500) ≈ 9 => 29 =512 ips reserved for each VLAN

Subnet Mask => 11111111.11111111.11111110.00000000 = 255.255.254.0

IP Range = 192.168.0.0 – 192.168.1.255 => VLAN1

IP Range= 192.168.2.0 - 192.168.3.255 => VLAN2

IP Range = 192.168.4.0 - 192.168.5.255 => VLAN3

This is an example configuration of dividing the total number of host required in different VLANs. Then by using the technique of VLSM (Variable Length Subnet Masking) we create subnets of our networks. As mentioned above we can also create subnets for all other branches and here are the subnets in the table below.

**LONDON IP’s (1500):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VLANS | Ip Range | Subnet Mask | Network Address | Broadcast Address | No# |
| VLAN 30 | 192.168.0.1 - 192.168.1.254 | 255.255.254.0 | 192.168.0.0 | 192.168.1.255 | 500 |
| VLAN 40 | 192.168.2.1 - 192.168.3.254 | 255.255.254.0 | 192.168.2.0 | 192.168.3.255 | 500 |
| VLAN 50 | 192.168.4.1 - 192.168.5.254 | 255.255.254.0 | 192.168.4.0 | 192.168.5.255 | 500 |

**LEICESTER IP’s (1200):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VLANS | Ip Range | Subnet Mask | Network Address | Broadcast Address | No# |
| VLAN 30 | 192.168.6.1 - 192.168.7.254 | 255.255.254.0 | 192.168.6.0 | 192.168.7.255 | 400 |
| VLAN 40 | 192.168.8.1 - 192.168.9.254 | 255.255.254.0 | 192.168.8.0 | 192.168.9.255 | 400 |
| VLAN 50 | 192.168.10.1 - 192.168.11.254 | 255.255.254.0 | 192.168.10.0 | 192.168.11.255 | 400 |

**LIVERPOOL IP’s (900):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VLANS | Ip Range | Subnet Mask | Network Address | Broadcast Address | No# |
| VLAN 30 | 192.168.12.1 - 192.168.13.254 | 255.255.254.0 | 192.168.12.0 | 192.168.13.255 | 300 |
| VLAN 40 | 192.168.14.1 - 192.168.15.254 | 255.255.254.0 | 192.168.14.0 | 192.168.15.255 | 300 |
| VLAN 50 | 192.168.16.1 - 192.168.17.254 | 255.255.254.0 | 192.168.16.0 | 192.168.17.255 | 300 |

**LEEDS IP’s (500):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VLANS | Ip Range | Subnet Mask | Network Address | Broadcast Address | No# |
| VLAN 30 | 192.168.18.1 - 192.168.18.254 | 255.255.255.0 | 192.168.18.0 | 192.168.18.255 | 200 |
| VLAN 40 | 192.168.19.1 - 192.168.19.254 | 255.255.255.0 | 192.168.19.0 | 192.168.19.255 | 150 |
| VLAN 50 | 192.168.20.1 - 192.168.20.254 | 255.255.255.0 | 192.168.20.0 | 192.168.20.255 | 150 |

# 

# 4. Switching & DHCP Implementation

## 4.1 VLAN Configuration

* VLAN segmentation using **Layer 2 switches**.
* **Trunk ports** configured for VLAN communication across switches.
* **Inter-VLAN routing** implemented using Layer 3 switches.

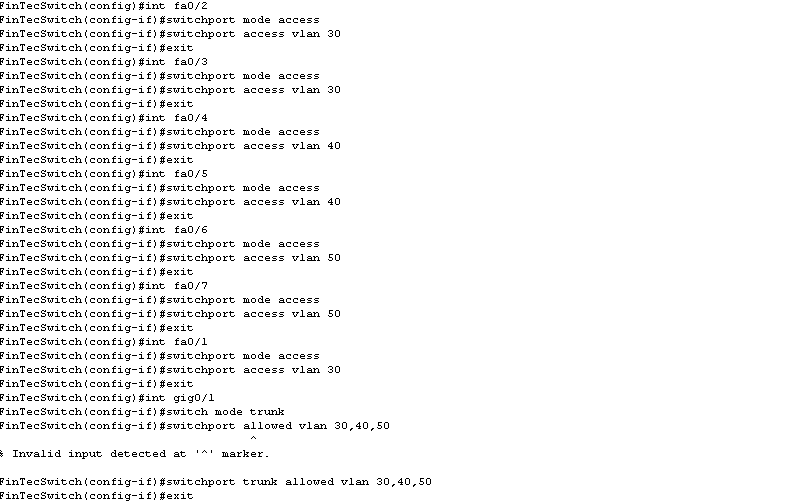
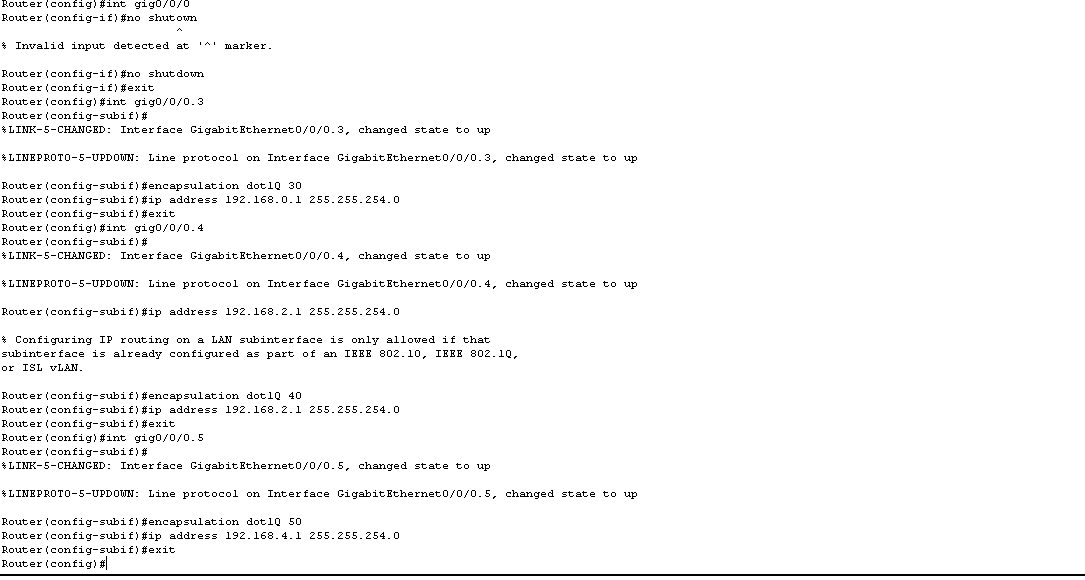


Figure 4.1 (Switchport VLAN)

**Inter-VLAN routing:**

**London Addresses & config:-**

****

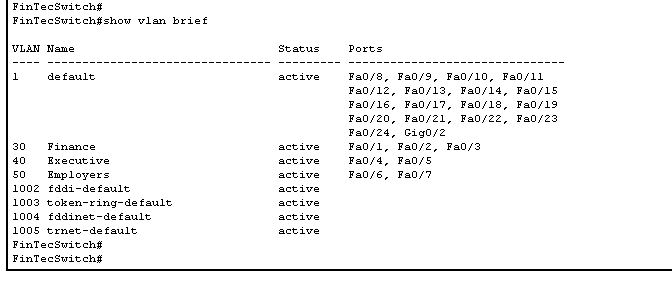
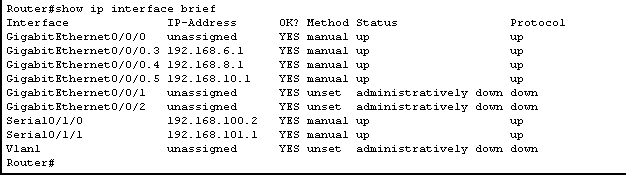
****

Figure 4.2 (Configuration)

**Leicester Addresses:-**

****

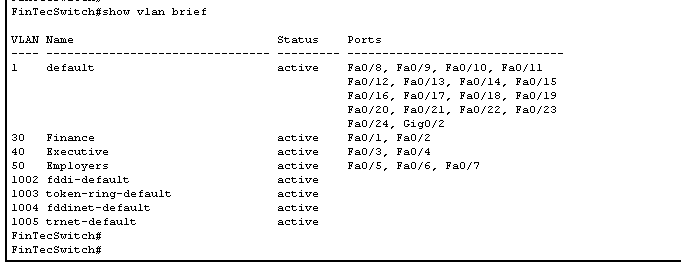
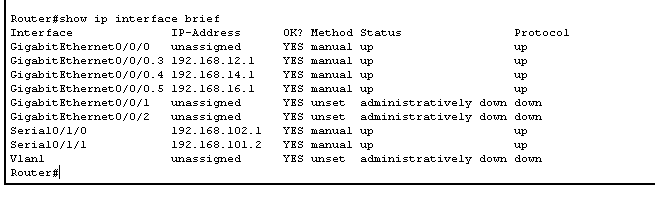


Figure 4.3 (Configuration)

**Liverpool Addresses:-**

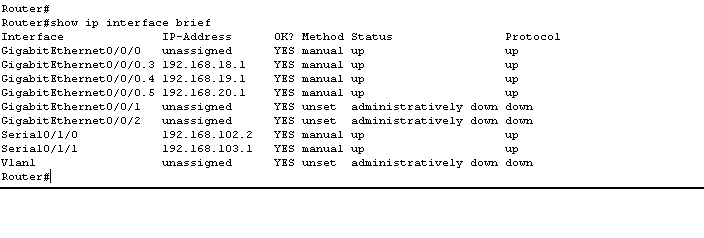
****

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4.4 (Configuration)

**Leeds Addresses:-**

****

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4.5 (Configuration)

**Trunking PORTs London**

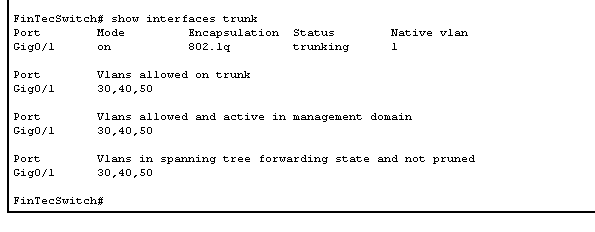


Figure 4.6 (Trunk)

**Trunking PORTs Leicester**

Figure 4.6 (Trunk)

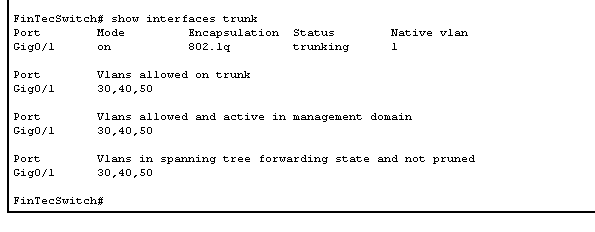


Figure 4.7 (Trunk)

**Trunking PORTs Liverpool**

A white screen with black text

AI-generated content may be incorrect.

Figure 4.8 (Trunk)

**Trunking PORTs Leeds**

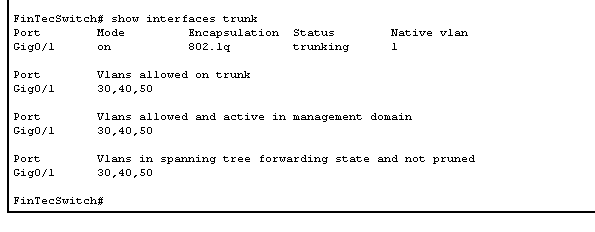


Figure 4.9 (Trunk)

## 4.2 DHCP Implementation

* **DHCP servers** will automatically assign IP addresses to VLANs.
* **Static reservations** for critical devices.
* Exclusion of reserved addresses to avoid conflicts.

**Example DHCP Configuration:**

**London DHCP Configuration:**

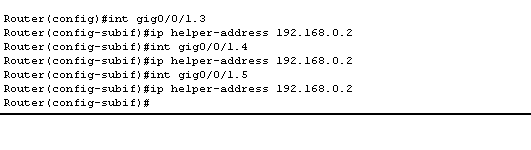
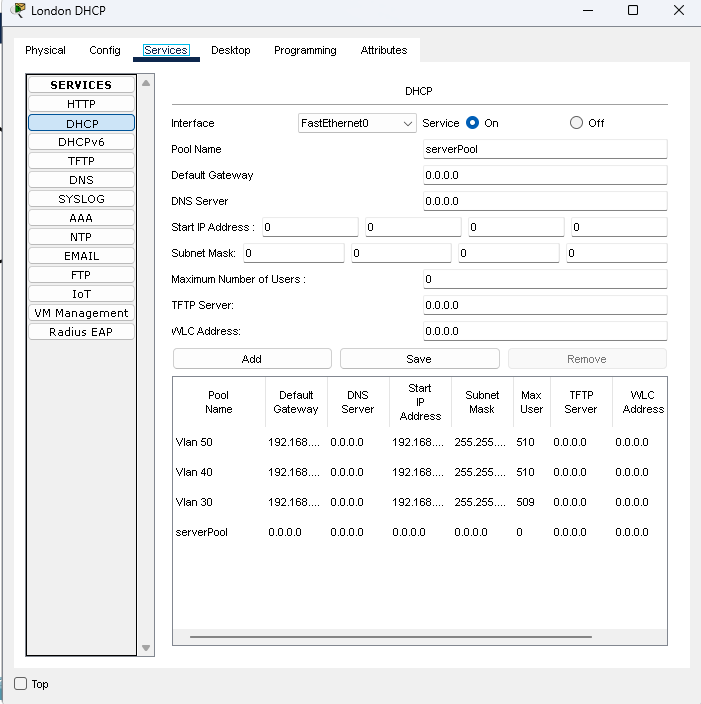
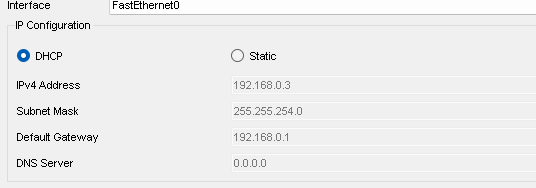


Figure 4.10 (DHCP Helper)





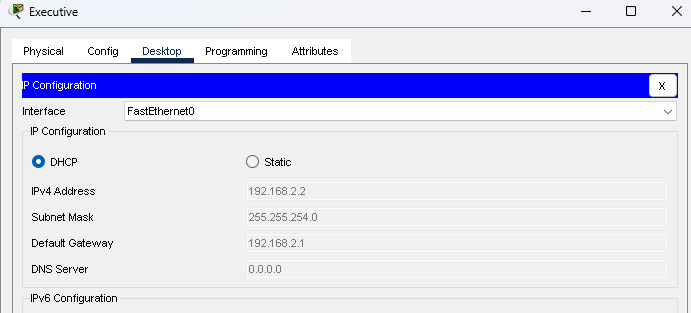
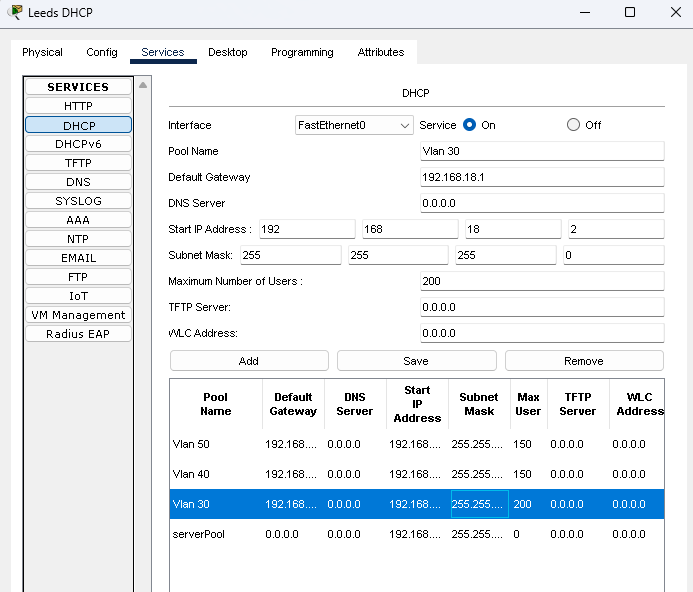
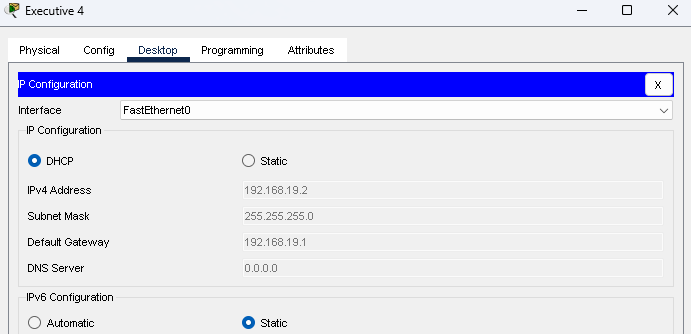


Figure 4.11 (DHCP Config)

Dynamic Host Configuration Protocol (Figure 4.10-4.11), more commonly referred as DHCP, is a protocol that routinely assigns addresses to devices on a network. Think of it as a pleasant host that gives out tickets to visitors at a large birthday celebration, ensuring everyone knows in which place to take a seat down. DHCP eliminates the want for guide address undertaking, making it simpler for brand spanking new gadgets to sign up for the community. It allows organize the community with the aid of giving every tool a completely unique identifier, permitting clean conversation. This automated technique saves time, reduces errors, and continues the network prepared and efficient. DHCP simplifies connectivity, ensuring dependable operation for all customers everywhere.

We have deployed DHCP servers to all the branches and they will provide IP addresses to all connected machines. The mention above example contains the London branch DHCP server containing all the IP addresses and in router we can define the IP of DHCP server that will give devices their IP addresses. Here is another example of Leeds branch of DHCP server.





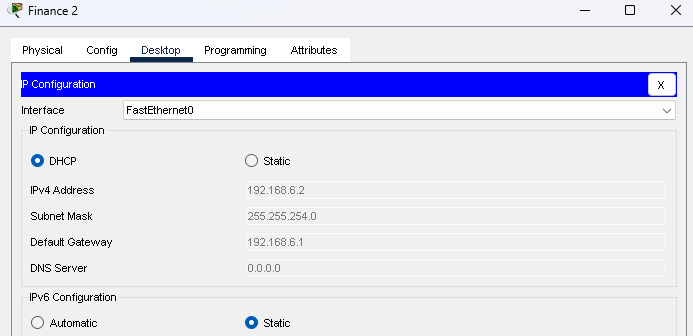
A screenshot of a computer

AI-generated content may be incorrect.

Figure 4.12 (DHCP Config)

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

Figure 4.13 (DHCP Config)

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4.14 (DHCP Config)

# 5. Network Security Implementation

## 5.1 Access Control & Security Policies

* **Access Control Lists (ACLs)** to block internet access for all non-London sites.
* **Role-based access control (RBAC)** to enforce user permissions.
* **VPN for secure remote access.**

**ACL Configuration Example:**

Access Control Lists, or ACLs, are simple rules of guidelines used to decide who can access precise traffic of a network or a digital device. Think of them as a listing of access and no access that acts like a safety gateway at the doorway of a building. ACLs help decide which gadgets or users are allowed to attach and which of them must be saved out, making sure that most effective the proper people advantage get admission to touchy facts. By placing these policies, ACLs provide an additional layer of protection, preserving networks safe, organized, and steady. This honest approach makes digital protection less difficult for every person.

We have represented ISP internet IP address as 1.1.1.2. We will apply AC Lists to ban this IP from sending packets or receiving packets in router configuration in three branches Leicester Leeds and Liverpool Router. Only London will have the Internet access from outside all the other branches will remain restricted from accessing internet connection.

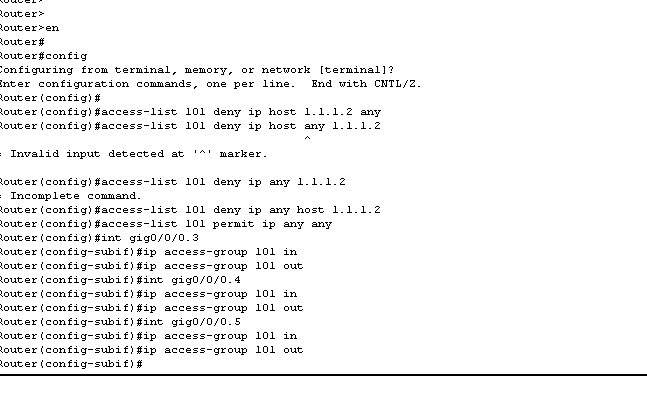


Figure 5.1 (Access List Blocking)

Here We applied Access Control List to deny IP 1.1.1.2 (Figure 5.1).

This is before Denying the Internet, see we can access internet if we ping the isp router.

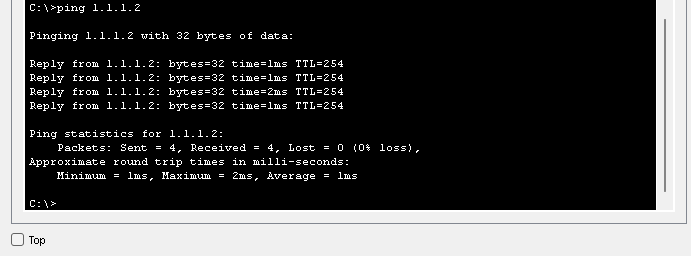


Figure 5.2 (Access List Testing)

And after applying ACL now we cannot access internet.

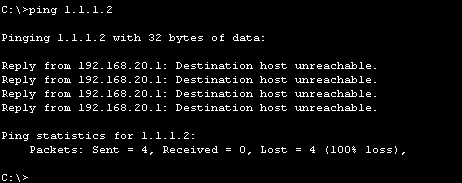


Figure 5.3 (Access List Testing)

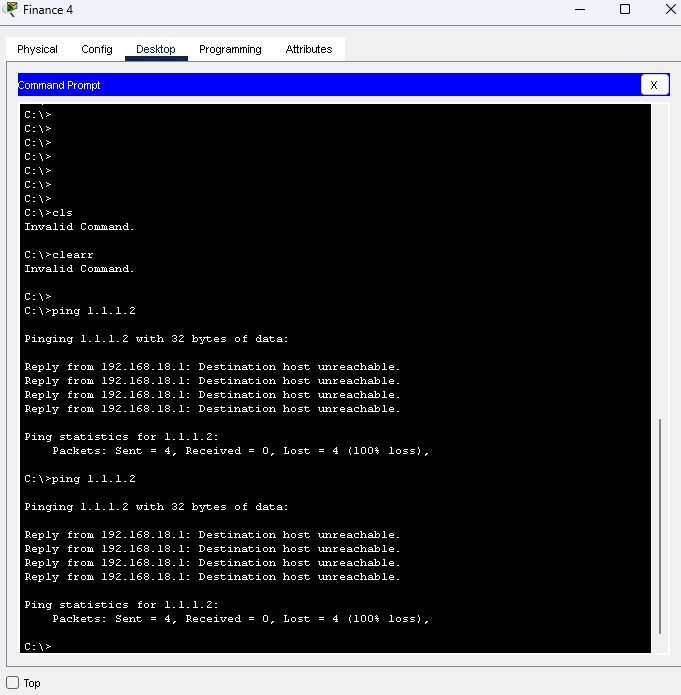


Figure 5.4 (Access List Testing)

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 5.5 (Access List Testing)

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5.6 (Access List Testing)

A computer screen shot of a computer program

AI-generated content may be incorrect.

Figure 5.7 (Access List Testing)

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 5.8 (Access List Testing)

A computer screen shot of a computer program

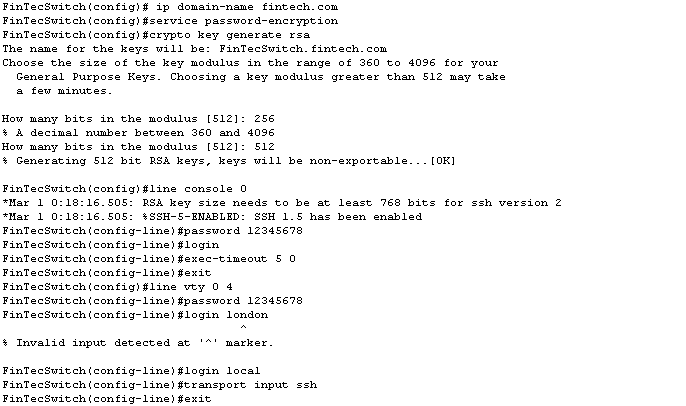
AI-generated content may be incorrect.

Figure 5.9 (Access List Testing)

## 5.2 Device Hardening Measures

* **SHA-256 password encryption** for routers and switches.
* **Disable Telnet** and enforce **SSH for secure remote management**.
* **Firewall implementation** to filter unauthorized traffic.

**Security Configuration Example:**



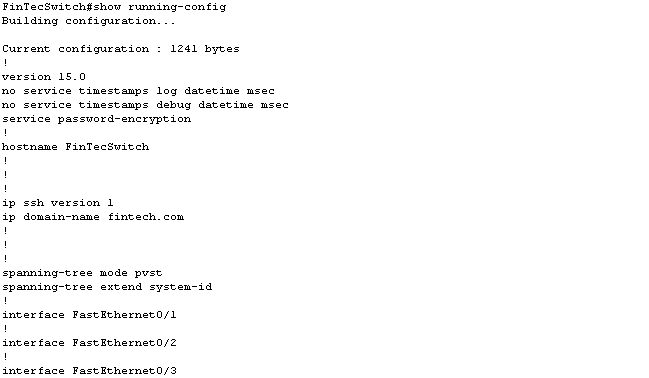




Figure 5.10 (Encrypting Switches)

These implementations was necessary to avoid unauthorized access to administrative functions of switches and routers.

**Encrypted Passwords on London Switch**

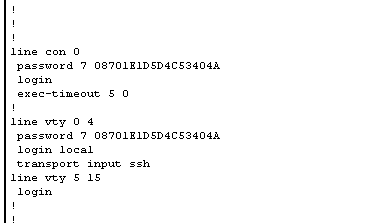


Figure 5.11 (Encrypting Passwords)

**Encrypted Passwords on Leicester Switch**

A computer screen shot of numbers and letters

AI-generated content may be incorrect.

Figure 5.12 (Encrypting Passwords)

**Encrypted Passwords on Liverpool Switch**

A computer screen shot of numbers and letters

AI-generated content may be incorrect.

Figure 5.13 (Encrypting Passwords)

**Encrypted Passwords on Leeds Switch**

A computer screen shot of numbers and letters

AI-generated content may be incorrect.

Figure 5.14 (Encrypting Passwords)

**Password Testing on all Switches**

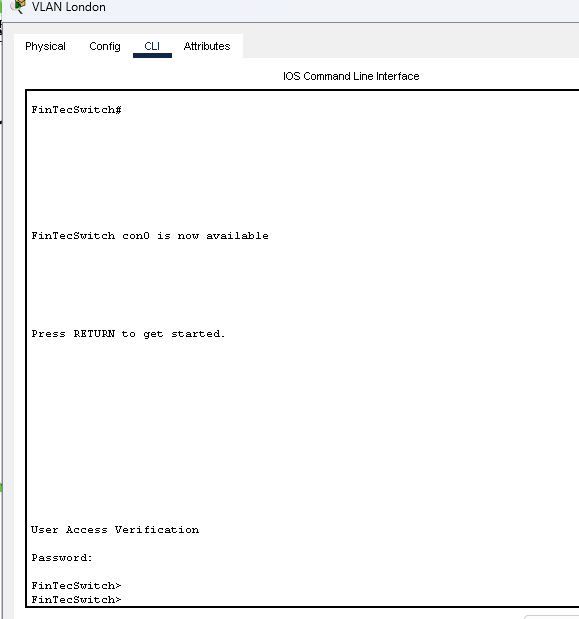


Figure 5.15 (Encrypting Password Testing)

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5.16 (Encrypting Password Testing)

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5.17 (Encrypting Password Testing)

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5.17 (Encrypting Password Testing)

# 6. Testing & Validation

## 6.1 Connectivity Testing

* **Ping and Traceroute commands** to verify network reachability.
* **OSPF neighbor verification** using CLI commands.
* VLAN connectivity tests to ensure proper segmentation.

Pinging devices:

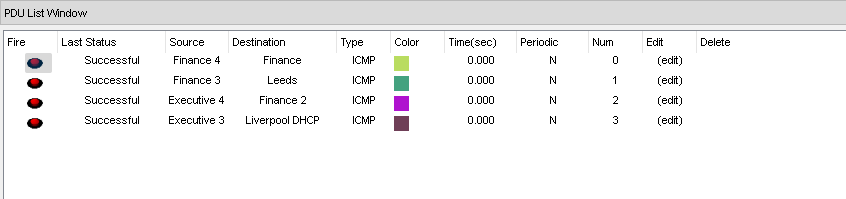


Figure 6.1 (ICMP ping test)

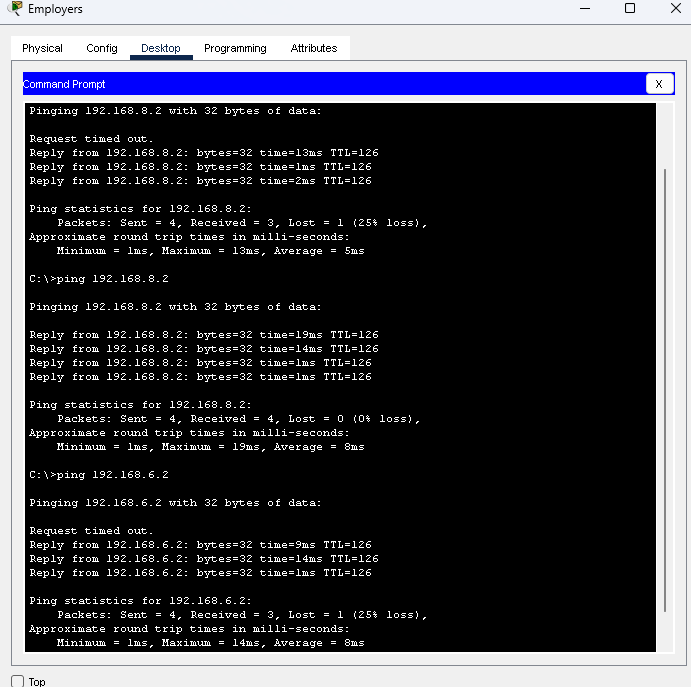


Figure 6.2 (ICMP ping test)

A computer screen shot of a program

AI-generated content may be incorrect.

Figure 6.2 (ICMP ping test)

OSPF Neighbour Verification:

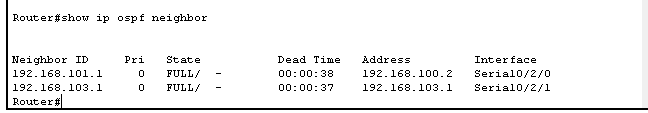


Figure 6.3 (OSPF Neighbour Test)

VLAN connectivity test:

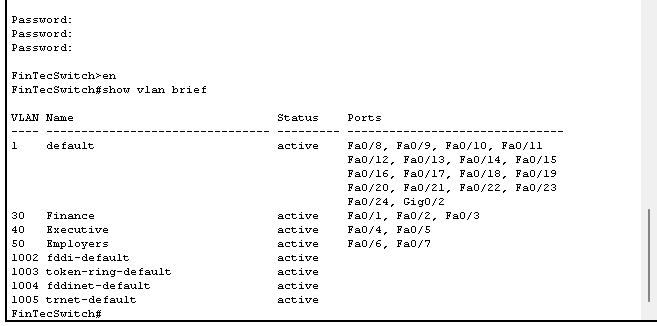


Figure 6.4 (VLAN Connectivity)

## 6.2 Security Testing

* **Penetration testing** to identify security vulnerabilities.
* **Simulated attacks** to validate firewall and ACL effectiveness.

# 7. Conclusion & Recommendations

The proposed network design for FinTech Inc. Efficiently fulfils the agency’s important necessities for scalability, protection, and operational efficiency. By leveraging OSPF for dynamic routing, VLANs for logical segmentation, and Access Control Lists (ACLs) for network filtering and coverage enforcement, the network guarantees streamlined data, go with the flow and stronger protection across departments. The inclusion of DHCP for automatic IP address control similarly simplifies management and reduces the chance of configuration mistakes.  
This architecture no longer only supports modern operational needs however is likewise built with future growth in thoughts. It lets in for the seamless integration of additional devices, customers, and services without compromising performance or protection. To elevate the network’s resilience and adaptability, future improvements may want to consist of cloud-based safety platforms, actual-time tracking structures, and the implementation of a 0-trust security version to limit internal and outside threats. Overall, the design represents a strong foundation for a secure, flexible, and scalable employer network capable of helping FinTech Inc.’s ongoing virtual transformation and innovation dreams.

# 

# 8. References

Jessie, 2022. Understanding Variable Length Subnet Masks (VLSM) [online]. Study CCNA. Available at: [https://study-ccna.com/variable-length-subnet-mask-vlsm/](https://study-ccna.com/variable-length-subnet-mask-vlsm/%20)

Anon., 2016. Configuring OSPF [online]. Cisco. Available at: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html%20)

Anon., 2022. DHCP and ACL [online]. Cisco Community. Available at: [https://community.cisco.com/t5/switching/dhcp-and-acl/td-p/4727760](https://community.cisco.com/t5/switching/dhcp-and-acl/td-p/4727760%20)

Anon., n.d. Inter-VLAN Routing: Configuration Examples [online]. Catchpoint. Available at: [https://www.catchpoint.com/network-admin-guide/inter-vlan-routing](https://www.catchpoint.com/network-admin-guide/inter-vlan-routing%20)

Cisco, 2023. VLAN Configuration Guide [online]. Cisco Docs. Available at: [https://www.cisco.com/c/en/us/td/docs/switches/lan/campus\_lan\_switches/vlan/configuration/guide/cli/b\_vlan\_cli.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/campus_lan_switches/vlan/configuration/guide/cli/b_vlan_cli.html%20)

Faircloth, J., 2014. Enterprise Applications Administration: The Definitive Guide to Implementation and Operations. 1st ed. Waltham: Syngress.

Maingi, B., 2022. Dynamic Host Configuration Protocol’s Security Issues and Recommendations Based on Systematic Review. [online] ResearchGate. Available at: <https://www.researchgate.net/publication/366867278_Dynamic_Host_Configuration_Protocol's_Security_Issues>

Zync Group, 2024. A Look at Cyber Attacks and Data Breaches in 2024 [online]. LinkedIn. Available at: <https://www.linkedin.com/pulse/look-cyber-attacks-data-breaches-2024-zyncgroup-9f9qe> .

Stallings, W., 2020. Network Security Essentials: Applications and Standards. 6th ed. Pearson Education.

ISO/IEC, 2018. ISO/IEC 27002:2018 - Information technology — Security techniques — Code of practice for information security controls. Geneva: International Organization for Standardization.