Contents

Introduction ............................................................................................................ 5

Network Topology Overview ...................................................................................... 5

Addressing table ...................................................................................................... 6

London ................................................................................................................ 7

Leeds .................................................................................................................. 7

Liverpool .............................................................................................................. 7

Leicester .............................................................................................................. 8

Routing ................................................................................................................... 8

OSPF-Routing Table: ............................................................................................. 8

Verifying OSPF configuration: .................................................................................... 9

R1-London ........................................................................................................... 9

Neighbour of R2: ................................................................................................. 10

Neighbour of R3: ................................................................................................. 10

Neighbour of R4: ................................................................................................. 11

Routing testing: ...................................................................................................... 11

Leeds – Liecester: ............................................................................................... 12

Leicester-Leeds: ................................................................................................. 12

Setting up Static with AD 120 Failback mechanism ................................................... 15

London .............................................................................................................. 15

Leicester ............................................................................................................ 15

Leeds ................................................................................................................ 15

Liverpool ............................................................................................................ 15

Verifying failover mechanism .................................................................................. 15

Configuring ABSR that advertise a default route in to the OSPF domain ...................... 16

Switching .............................................................................................................. 17

VLAN Design and Implementation ....................................................................... 17

Assigning Vlan on each site: ................................................................................ 18

Assign Vlan to access port ................................................................................... 18

Router-on-a-Stick Sub interface Setup per Router .................................................... 18

London .............................................................................................................. 18

Leicester ............................................................................................................ 19 Leeds ................................................................................................................ 19

Liverpool ............................................................................................................ 19

Trunking ................................................................................................................ 22

DHCP settings ....................................................................................................... 23

DHCP Testing ......................................................................................................... 25

London Area ....................................................................................................... 25

Leicester Area .................................................................................................... 26

Liverpool Area .................................................................................................... 26

Leeds Area ......................................................................................................... 27

DHCP Verification ............................................................................................... 28

Ping Testing ........................................................................................................... 29

London area ....................................................................................................... 29

Leeds area ......................................................................................................... 29

Liverpool area ..................................................................................................... 29

Leicester area ..................................................................................................... 30

Security ................................................................................................................. 30

London,Router ................................................................................................... 30

Switch ............................................................................................................... 31

Leicester ............................................................................................................ 31

Switch ............................................................................................................... 32

Leeds ................................................................................................................ 32

Switch ............................................................................................................... 33

Liverpool ............................................................................................................ 33

Switch ............................................................................................................... 34

Security Verification: .............................................................................................. 34

London .............................................................................................................. 34

Leeds ................................................................................................................ 35

Liverpool ............................................................................................................ 36

Leicester ............................................................................................................ 37

Verifying Security of Open Ports .............................................................................. 38

London .............................................................................................................. 38

Leeds ................................................................................................................ 39 Liverpool ............................................................................................................ 40

Leicester ............................................................................................................ 41

ACL ....................................................................................................................... 42

Final view .............................................................................................................. 46

Summary .............................................................................................................. 46

References ............................................................................................................ 48

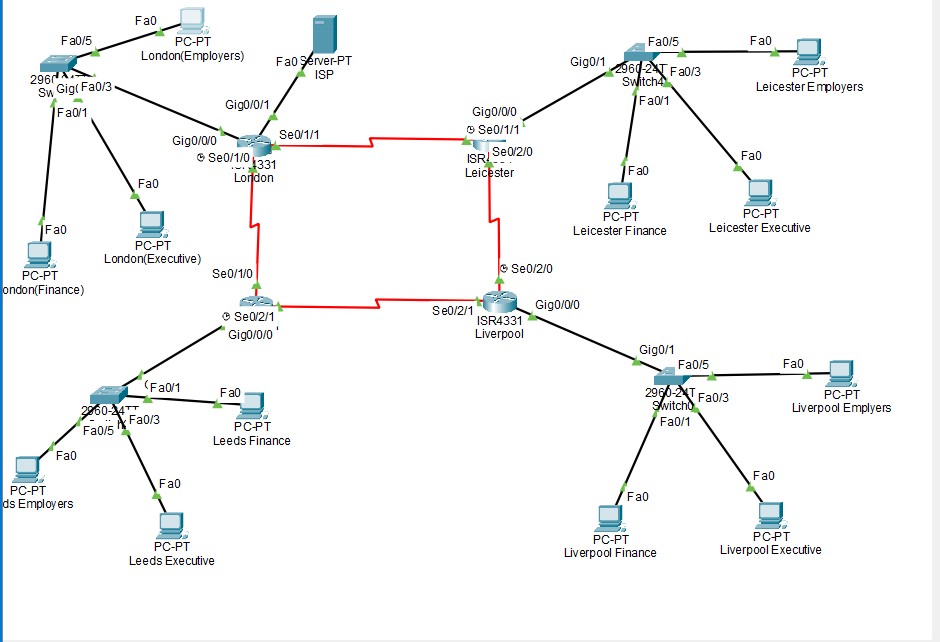
# Introduction

This report outlines the design and implementation of a secure, scalable enterprise network across four sites: London, Leicester, Liverpool, and Leeds. The network incorporates OSPF routing with static fallback, VLAN segmentation, DHCP for dynamic IP allocation, and ACLs for internet access control. Additional security measures, such as password encryption, port security, and SSH access, were applied to all routers and switches. The objective was to build a reliable and efficient infrastructure that ensures traffic isolation, failover resilience, and compliance with modern network security practices. Configuration steps were tested and validated, with screenshots provided as evidence throughout the report.

# Network Topology Overview

The network is designed to support a multi-site enterprise architecture across four locations: London, Leicester, Liverpool, and Leeds. Each site operates as a branch within the wider organizational structure and is inter-connected using serial links with dynamic and static routing for redundancy.

The design implements a hierarchical network topology with a focus on scalability, security, and efficient traffic segmentation. The topology integrates Layer 2 switching and Layer 3 routing, using technologies such as VLANs, Inter-VLAN routing (Router-on-aStick), DHCP, OSPF, and Access Control Lists (ACLs) to ensure both functionality and control.London serves as the central site and hosts the only internet connection in the network. All internet-bound traffic is routed through London via the GigabitEthernet0/0/1 interface. Access to the internet is restricted using ACLs to ensure that only devices within the London network have outbound internet access, in compliance with the organization's cybersecurity policies.



*Figure 1 – Topology*

# Addressing table

The network design utilizes Variable Length Subnet Masking (VLSM) to allocate IP space based on actual host requirements across different sites. This method enhances address efficiency, minimizes waste, and supports structured routing by assigning distinct subnets to each location and VLAN. Such an approach aligns with best practices for scalable and organized network architectures (Serpanos and Wolf, 2011).

## London

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| R1 – Router | G0/0/0 | 192.168.1.1 | 255.255.255.0 |
|  |  |  |  |
|  | S0/1/0 | 10.30.1.1 | 255.255.255.252 |
|  | S0/1/1 | 10.30.2.1 | 255.255.255.252 |
| Switch-London | VLAN 30 (Finance) | 192.168.10.2 | 255.255.255.0 |
|  | VLAN 40 (Exec) | 192.168.20.2 | 255.255.255.0 |
|  | VLAN 50 (Employ) | 192.168.30.2 | 255.255.255.0 |
| PC1–London | NIC | DHCP | Assigned via VLAN 30 |
| PC2–London | NIC | DHCP | Assigned via VLAN 40 |
| PC3–London | NIC | DHCP | Assigned via VLAN 50 |

## Leeds

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| R3 – Router | G0/0/0 | 192.168.4.1 | 255.255.255.0 |
|  | S0/2/1 | 10.30.4.2 | 255.255.255.252 |
|  | S0/1/0 | 10.30.1.2 | 255.255.255.252 |
| Switch-Leeds | VLAN 30 | 192.168.130.2 | 255.255.255.0 |
|  | VLAN 40 | 192.168.140.2 | 255.255.255.0 |
|  | VLAN 50 | 192.168.150.2 | 255.255.255.0 |
| PC1–Leeds | NIC | DHCP | Assigned via VLAN 30 |
| PC2–Leeds | NIC | DHCP | Assigned via VLAN 40 |
| PC3–Leeds | NIC | DHCP | Assigned via VLAN 50 |

## Liverpool

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| R4 – Router | G0/0/0 | 192.168.3.1 | 255.255.255.0 |
|  | S0/2/1 | 10.30.4.1 | 255.255.255.252 |
|  | S0/2/0 | 10.30.3.2 | 255.255.255.252 |
| Switch-Liverpool | VLAN 30 | 192.168.100.2 | 255.255.255.0 |
|  | VLAN 40 | 192.168.110.2 | 255.255.255.0 |
|  | VLAN 50 | 192.168.120.2 | 255.255.255.0 |
| PC1–Liverpool | NIC | DHCP | Assigned via VLAN 30 |
| PC2–Liverpool | NIC | DHCP | Assigned via VLAN 40 |
| PC3–Liverpool | NIC | DHCP | Assigned via VLAN 50 |

## Leicester

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| R2 – Router | G0/0/0 | 192.168.2.1 | 255.255.255.0 |
|  | S0/2/0 | 10.30.3.1 | 255.255.255.252 |
|  | S0/1/1 | 10.30.2.2 | 255.255.255.252 |
| Switch-Leicester | VLAN 30 | 192.168.40.2 | 255.255.255.0 |
|  | VLAN 40 | 192.168.50.2 | 255.255.255.0 |
|  | VLAN 50 | 192.168.60.2 | 255.255.255.0 |
| PC1–Leicester | NIC | DHCP | Assigned via VLAN 30 |
| PC2–Leicester | NIC | DHCP | Assigned via VLAN 40 |
| PC3–Leicester | NIC | DHCP | Assigned via VLAN 50 |

# Routing

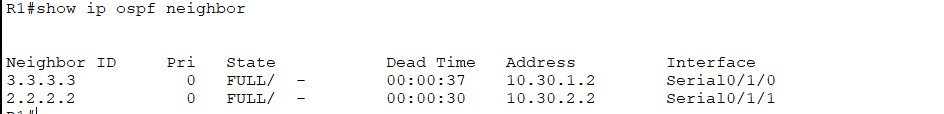
To establish resilient and adaptive inter-site communication, the network employs the Open Shortest Path First (OSPF) protocol in a single-area configuration (Area 0). OSPF was chosen for its rapid convergence, hierarchical design support, and efficient link-state operations, making it ideal for multi-branch enterprise networks (Lai et al., 2008). In addition to OSPF, static routes with higher administrative distances are configured as a fallback solution, ensuring uninterrupted connectivity in the event of dynamic route failure. This hybrid routing strategy improves both reliability and control (Medhi and Ramasamy, 2007).

OSPF-Routing Table:

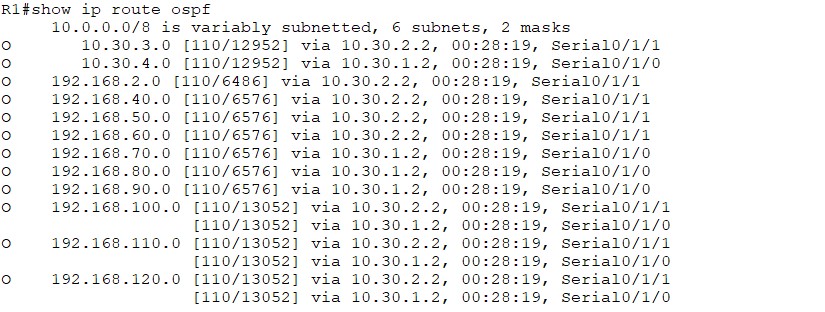
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Router | OSPF  Process ID | Router ID | Networks Advertised | Passive Interfaces |
| R1 – London | 1 | 1.1.1.1 | 192.168.1.0/24 | R1 – London |
|  |  |  | 10.30.1.0/30 |  |
|  |  |  | 10.30.2.0/30 |  |
| R2 – Leicester | 1 | 2.2.2.2 | 192.168.2.0/24 | G0/0/0,  Loopback0 |
|  |  |  | 10.30.2.0/30 |  |
|  |  |  | 10.30.3.0/30 |  |
| R3 – Leeds | 1 | 3.3.3.3 | 192.168.3.0/24 | G0/0/0,  Loopback0 |
|  |  |  | 10.30.1.0/30 |  |
|  |  |  | 10.30.4.0/30 |  |
|  |  |  | 192.168.70.0/24 |  |
|  |  |  | 192.168.80.0/24 |  |
|  |  |  | 192.168.90.0/24 |  |
| R4 – Liverpool | 1 | 4.4.4.4 | 192.168.4.0/24 | G0/0/0,  Loopback0 |
|  |  |  | 10.30.3.0/30 |  |
|  |  |  | 10.30.4.0/30 |  |
|  |  |  | 192.168.100.0/24 |  |
|  |  |  | 192.168.110.0/24 |  |
|  |  |  | 192.168.120.0/24 |  |

Verifying OSPF configuration:

## R1-London

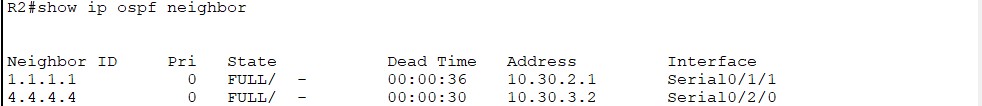


*Figure 2*



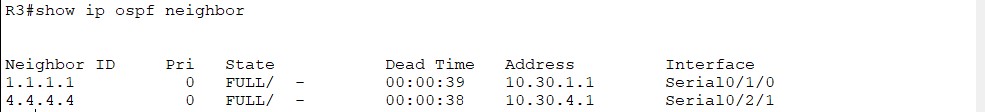
*Figure 3*

Neighbour of R2:

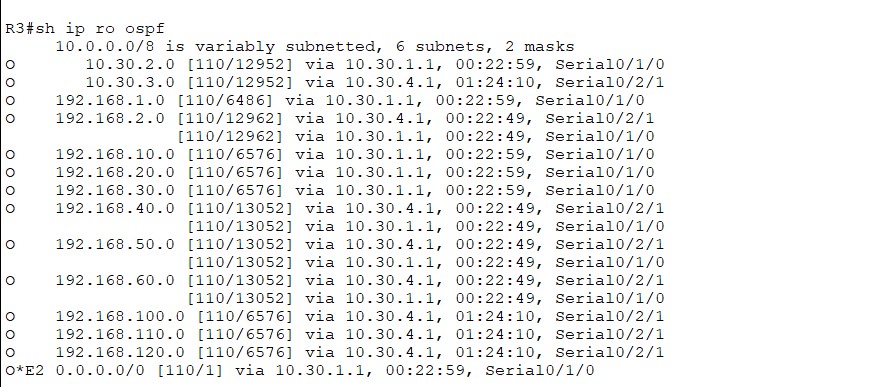


*Figure 4*

Neighbour of R3:

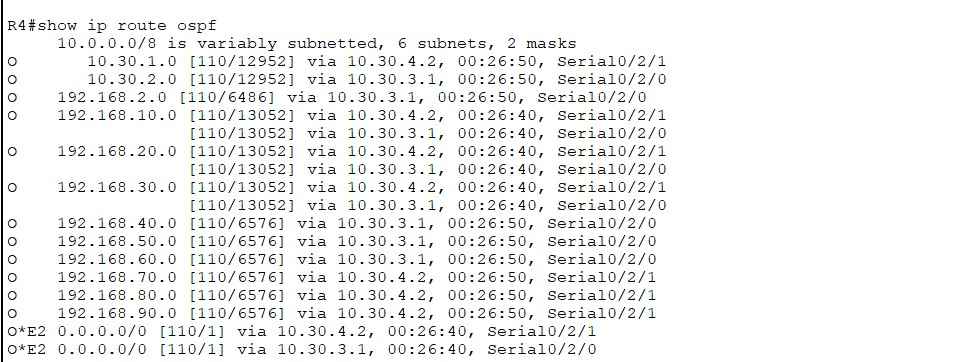
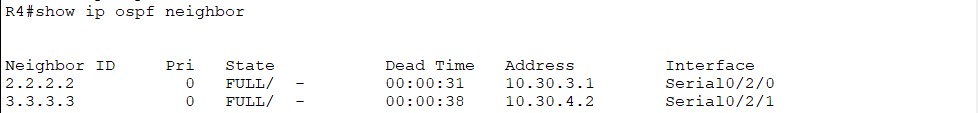


*Figure 5*



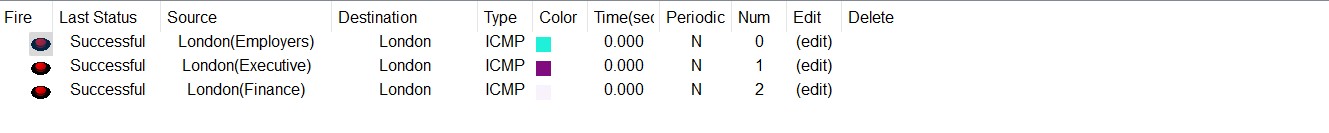
*Figure 6*

Neighbour of R4:

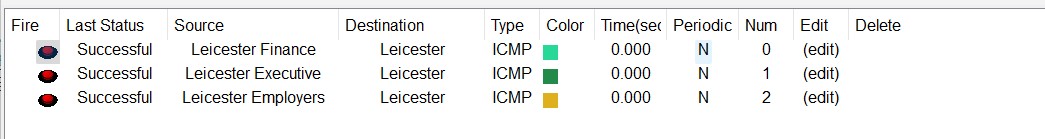


*Figure 7*

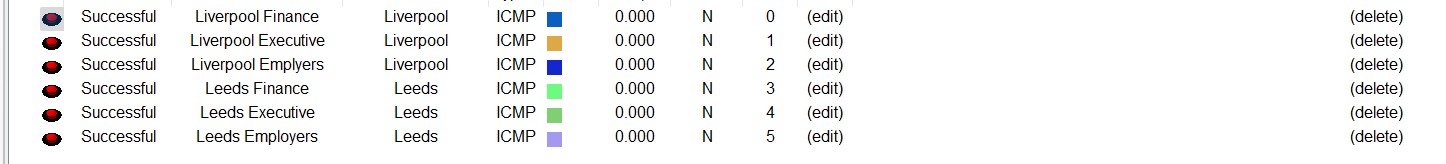
Routing testing:



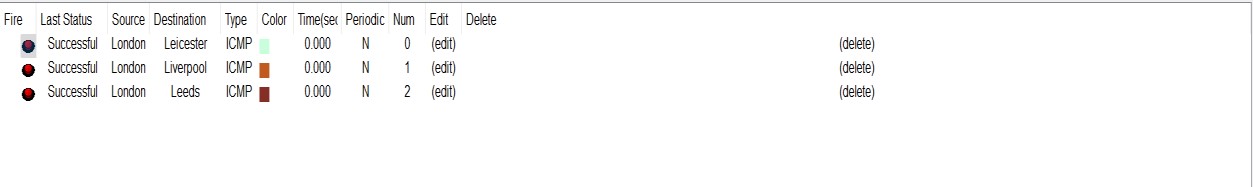
*Figure 8:Successful ping between devices and router London*



*Figure 9Successful ping between devices and router Leicester*

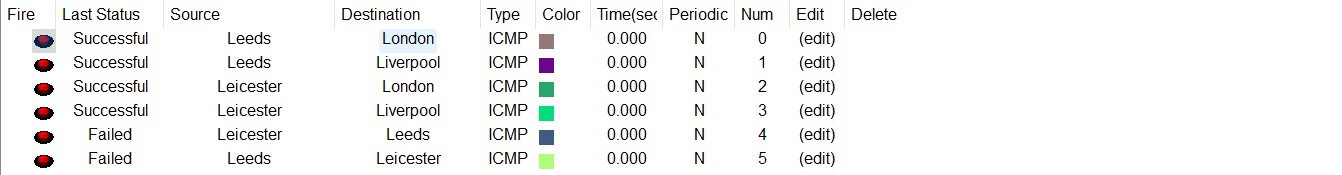


*Figure 10Successful ping between devices and router Liverpool ////<< Successful ping between devices and router Leeds>>*



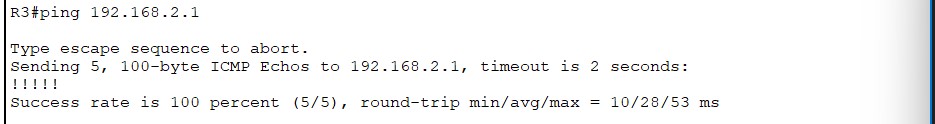
*Figure 11*

Connectivity between the routers at Leeds (R3) and Leicester (R2) was verified using ICMP ping tests. As evidenced by the test results, the ping from Leeds to Leicester’s gateway IP address (192.168.2.1) and vice versa (192.168.70.1) achieved a 100% success rate, confirming stable two-way communication. Although the simulation panel initially showed failed attempts, these were resolved after finalizing OSPF and interface configurations. This confirms that dynamic routing between the two sites is fully operational



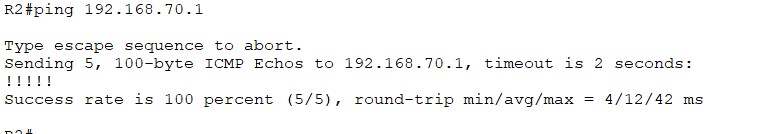
*Figure 12*

Leeds – Liecester:

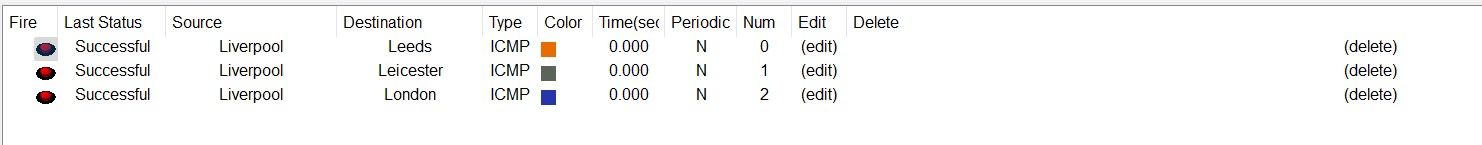


*Figure 13*

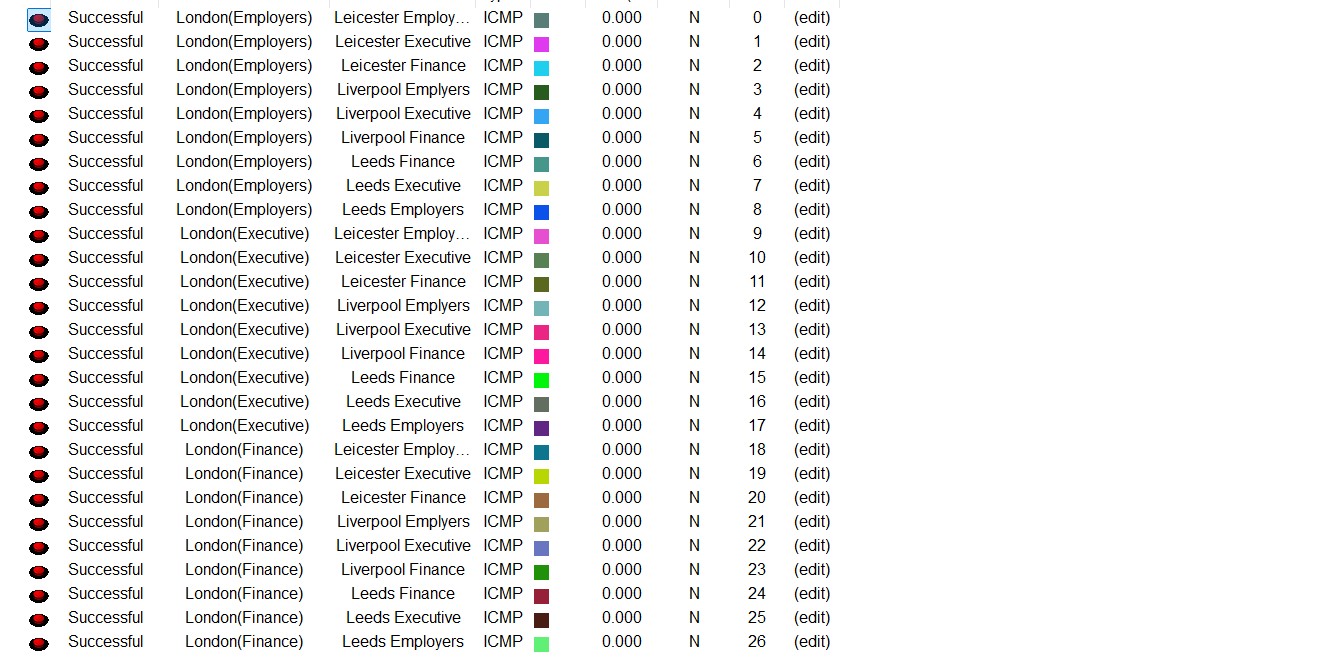
Leicester-Leeds:



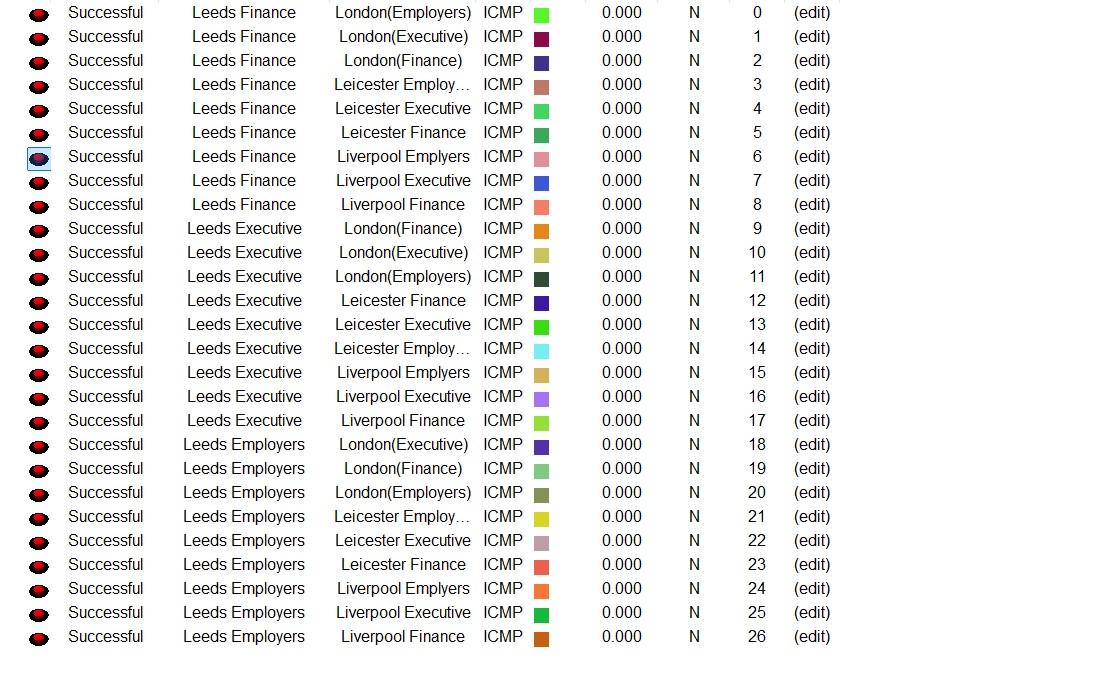
*Figure 14*



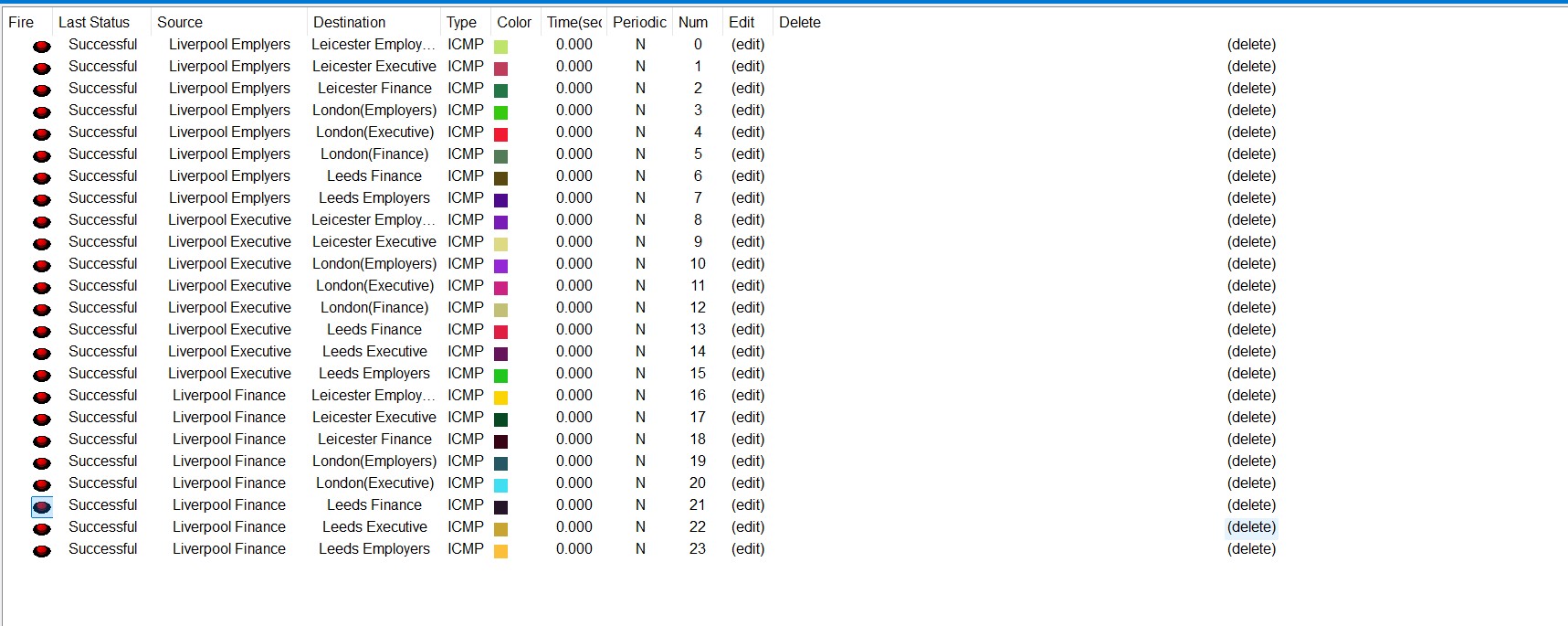
*Figure 15*



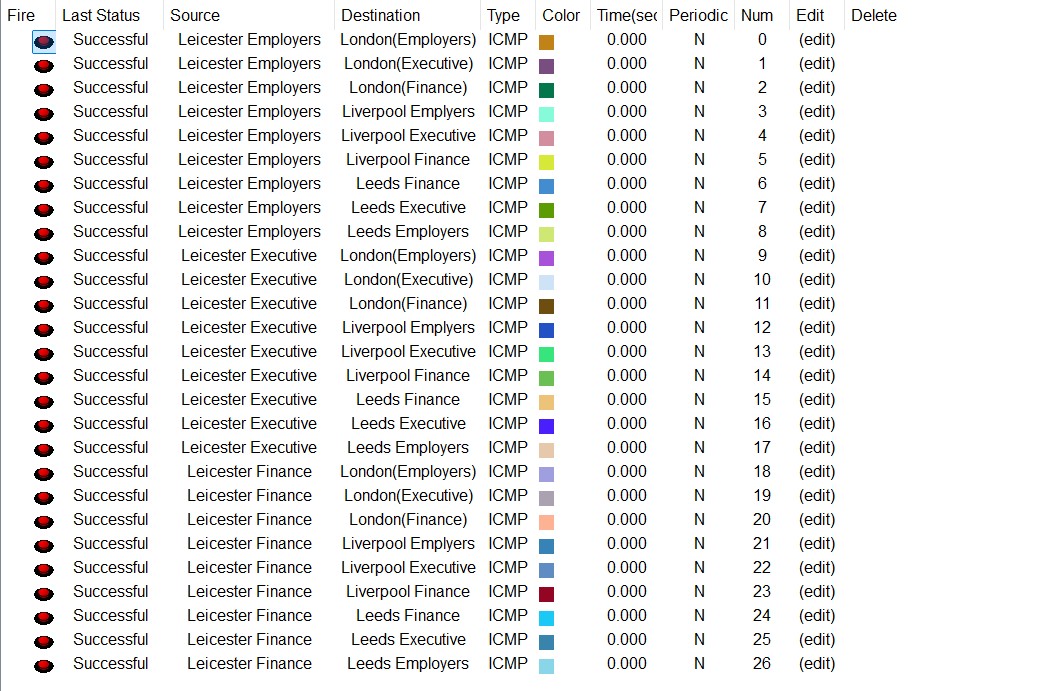
*Figure 16 Successful ping between London devices and other devices*



*Figure 17 Successful ping between Leeds devices and other devices*



*Figure 18 Successful ping between Liverpool devices and other devices*

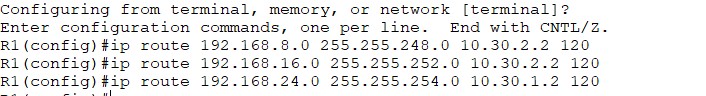


*Figure 19 Successful ping between Leicester devices and other devices*

To validate end-to-end connectivity across the network, PC-to-PC ping tests were conducted between sites. Each device successfully obtained an IP address via DHCP, and the ping responses confirmed that inter-VLAN routing and OSPF-based communication were functioning correctly. As explained by Gavin, ping serves as a fundamental diagnostic tool to test connectivity between devices and ensure network reachability. The successful test results demonstrate that all configured hosts are fully reachable across the WAN, confirming the reliability of the overall network design.

# Setting up Static with AD 120 Failback mechanism

## London



*Figure 20*

## Leicester



*Figure 21*

## Leeds



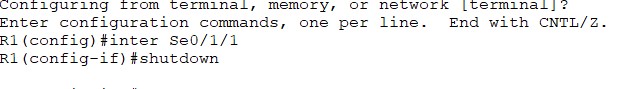
*Figure 22*

## Liverpool

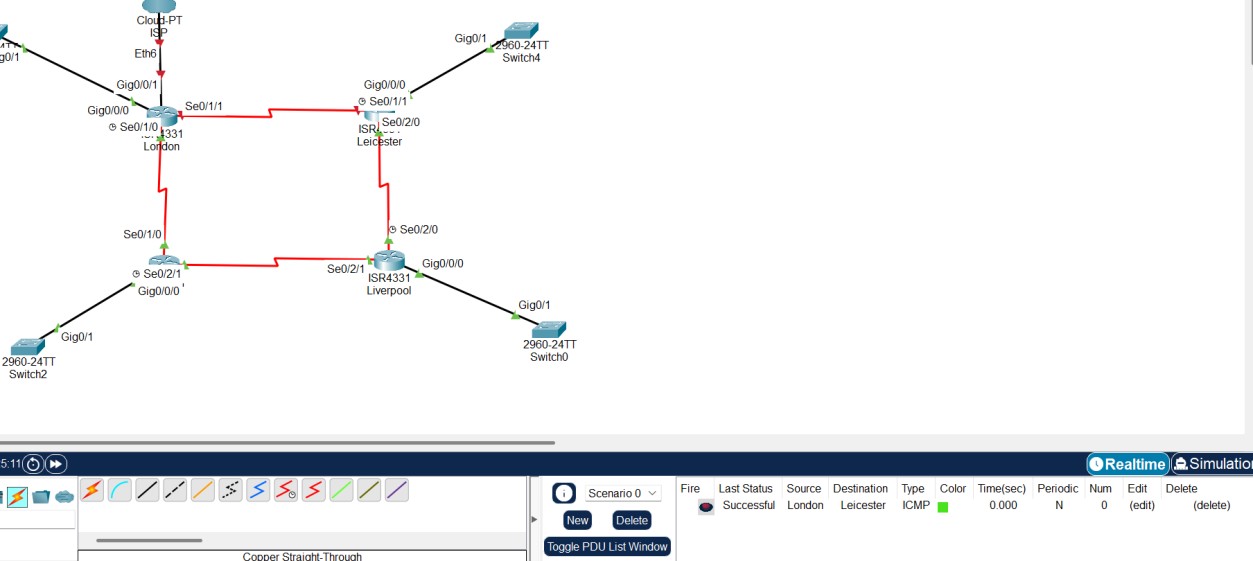


*Figure 23*

# Verifying failover mechanism



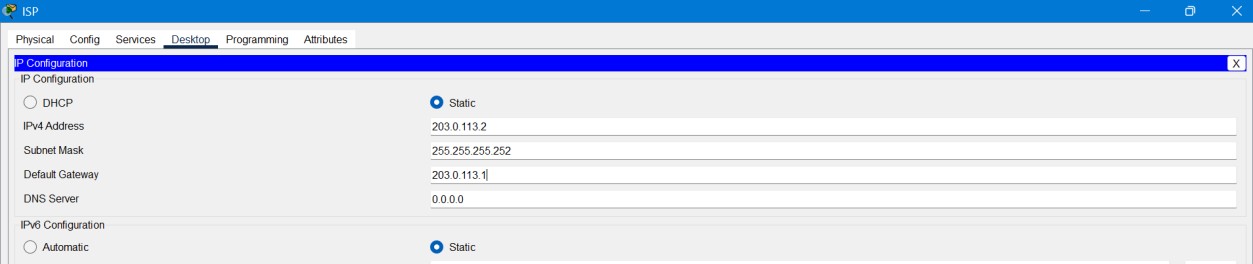
*Figure 24*



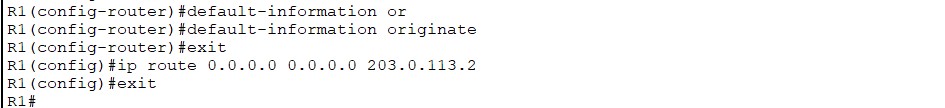
*Figure 25*

To validate the fallback routing mechanism, a primary link between London and Leicester was intentionally disabled using The shutdown command on interface Serial0/1/1 of the London router. Following this action, ICMP traffic was still successfully routed from London to Leicester, confirming that OSPF dynamically recalculated the best available path via the alternative route through Liverpool. This behavior confirms that the failover routing setup is functioning as intended, ensuring uninterrupted connectivity even during link failures.

# Configuring ABSR that advertise a default route in to the OSPF domain

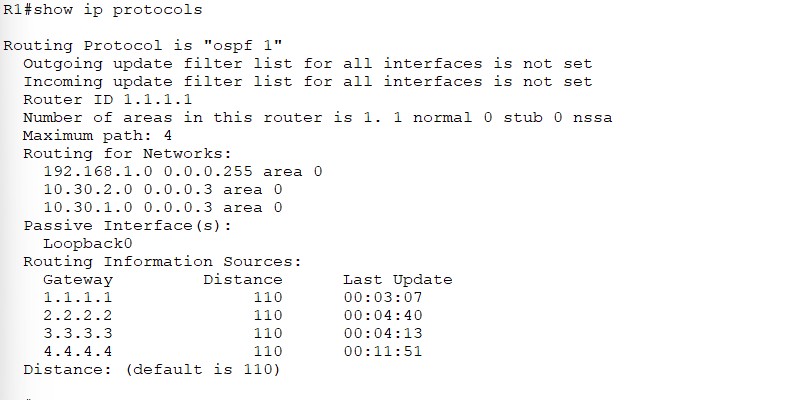
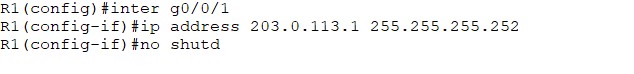


*Figure 26Figure 27*



*Figure 28*

*Figure 29*



*Figure 30*

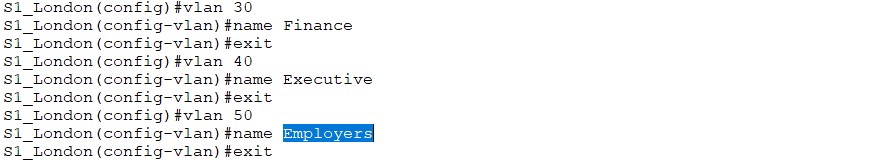
Implementing ABRSP helps protect the routers that connect different parts of the network or link it to the internet. These routers play a key role in sharing routing information, so securing them prevents fake or harmful routes from getting in. It’s a smart way to keep the network stable and safe, especially when advertising default routes.

# Switching

## VLAN Design and Implementation

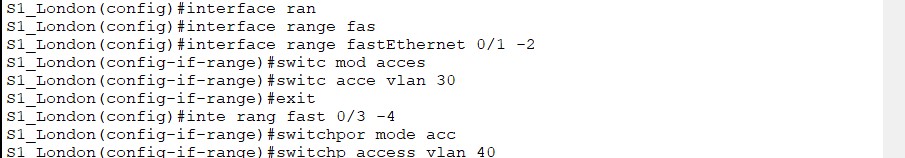
Virtual LANs (VLANs) were implemented to logically segment network traffic, improving both security and performance by isolating departments such as Finance, Executive, and Employers into VLANs 30, 40, and 50 respectively (Cisco, n.d.). At the London site, VLANs were assigned to specific FastEthernet ports—0/1-2 for Finance, 0/3-4 for Executive, and 0/5-6 for Employers—with each configured in access mode to prevent VLAN hopping. Router-on-a-Stick configuration was used to enable inter-VLAN communication and DHCP services via sub-interfaces. This standardized VLAN setup was consistently applied across Leicester, Liverpool, and Leeds to maintain scalability and centralized policy control.

Assigning Vlan on each site:

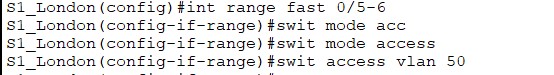


*Figure 31*

## Assign Vlan to access port



*Figure 32*



*Figure 33*

# Router-on-a-Stick Sub interface Setup per Router

## London



*Figure 34*

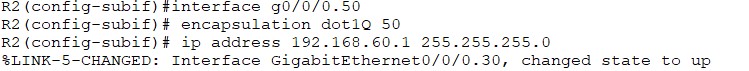


*Figure 35s*



*Figure 36*

## Leicester



*Figure 37*

## Leeds





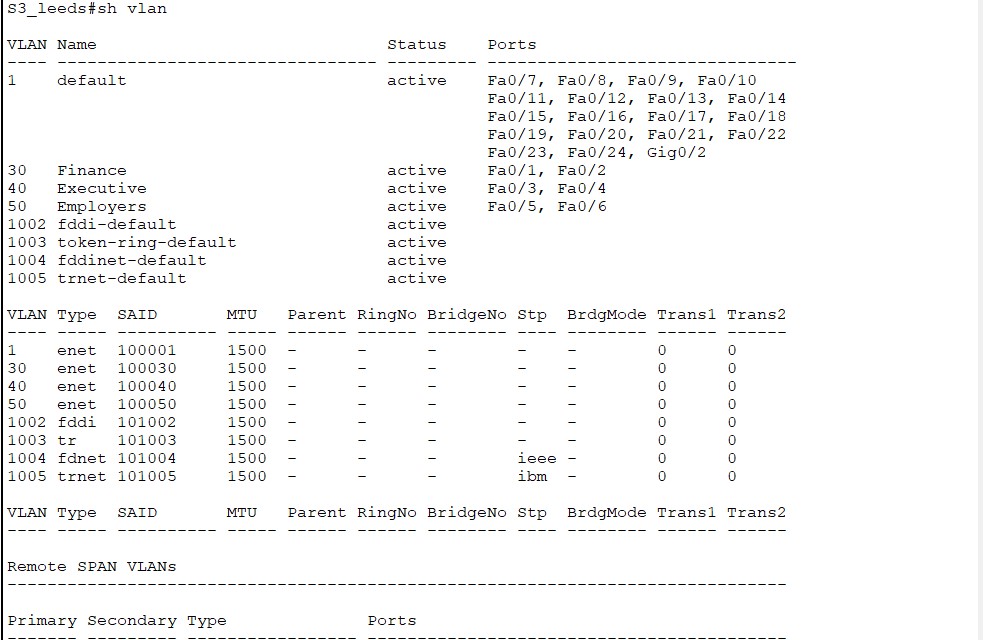
*Figure 38*

## Liverpool

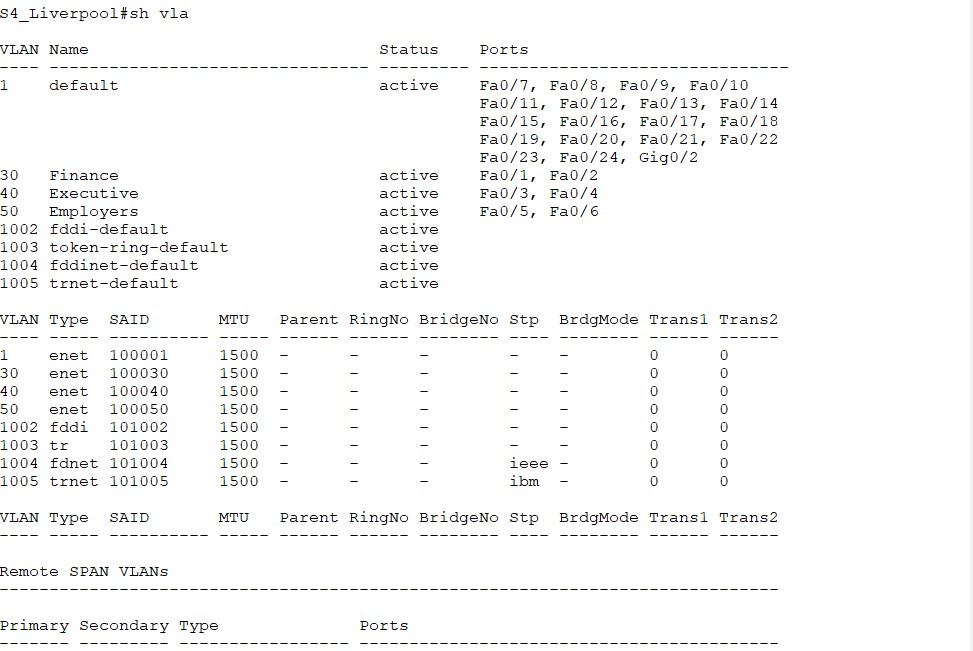


*Figure 39*

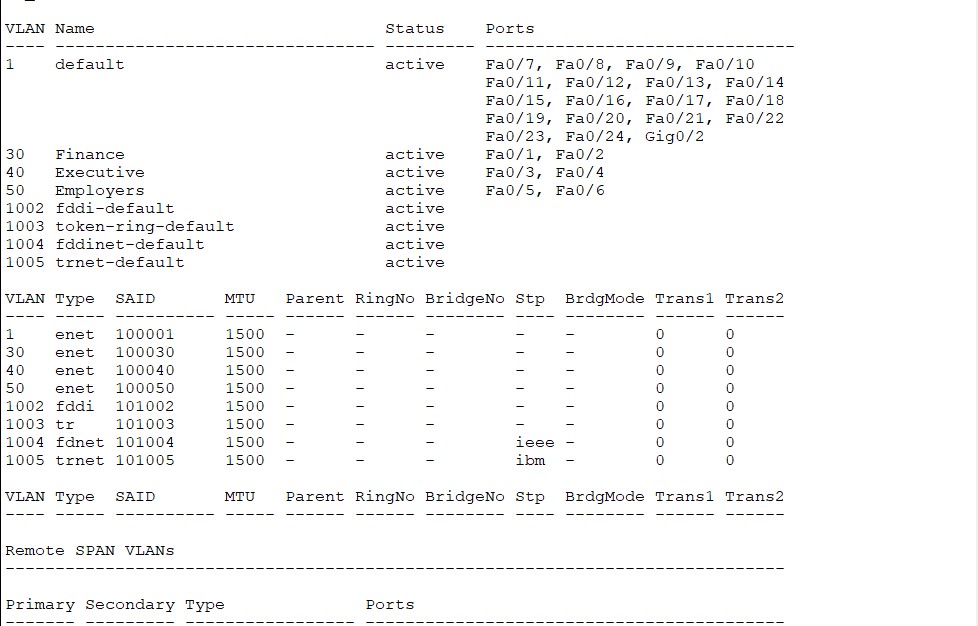
*Figure 40*



*Figure 41*



*Figure 42*



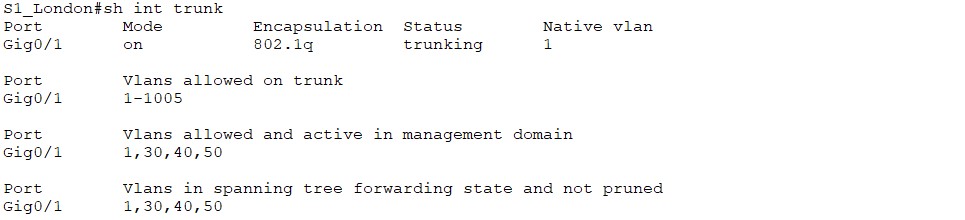
*Figure 43*

The successful creation and port assignment of VLANs at each site were verified using the show vlan command on the switches. The output confirmed that VLANs 30, 40, and 50 were correctly created and associated with their designated access ports at London, Leicester, Liverpool, and Leeds. As highlighted by Sun et al. (2014), proper VLAN segmentation and verification help ensure isolated traffic domains and reduce broadcast congestion, contributing to more secure and efficient network operation.

# Trunking

Trunking is essential on Layer 2 switches to enable communication between multiple VLANs over a single physical link. In a router-on-a-stick setup, trunk ports forward tagged traffic from all VLANs to the router’s sub-interfaces for inter-VLAN routing. Without trunking,

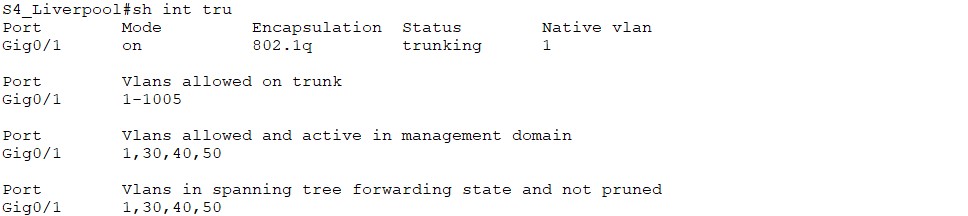
VLANs would remain isolated, preventing access to shared resources or centralized services (Aziz).



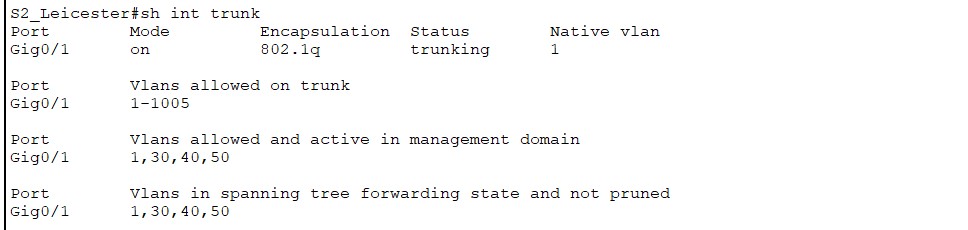
*Figure 44*



*Figure 45*



*Figure 46*

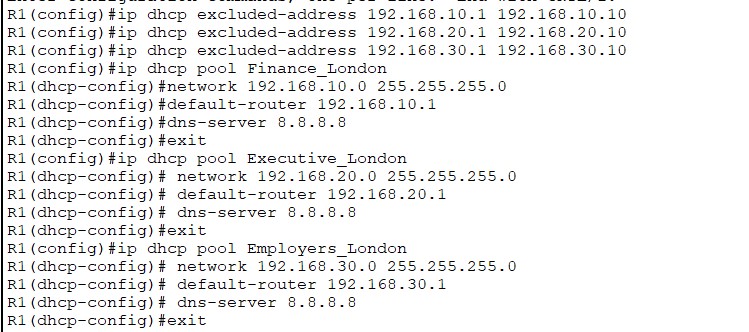


*Figure 47Figure 48*

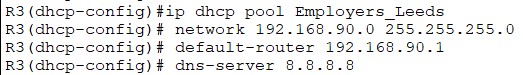
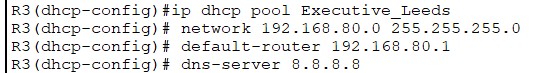
To enable inter-VLAN communication, trunking was configured on the switch port connecting to the router using IEEE 802.1Q encapsulation. This allows multiple VLANs to traverse a single physical link by tagging traffic with VLAN identifiers. The "show interfaces trunk" command was used to verify trunk status. The output confirmed that Gig0/1 was actively trunking with VLANs 30, 40, and 50 allowed and forwarding. This setup is crucial for supporting the router-on-a-stick design and ensuring seamless VLANbased segmentation across the network (Aziz).

# DHCP settings

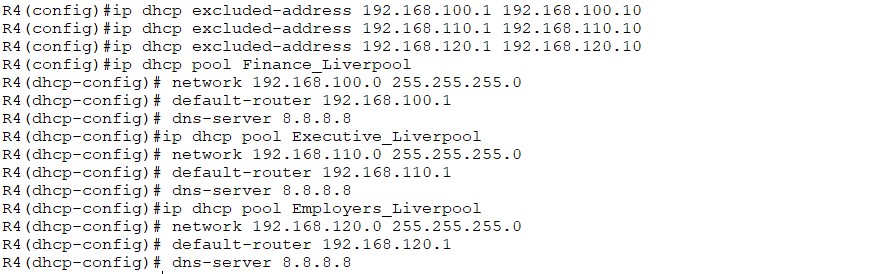
“Dynamic Host Configuration Protocol (DHCP) plays a critical role in simplifying IP address management, particularly in networks with a large number of devices. Rather than manually assigning IP addresses to each device, DHCP automates this process, ensuring efficient and error-free address allocation. For example, when a new desktop joins the network, it broadcasts a discovery message to locate available DHCP servers. A server, such as dhcpserve, responds with an appropriate IP address, subnet mask, default gateway, and DNS information. The desktop then confirms the offer, and the server finalizes the lease, preventing IP conflicts and ensuring reliability. This structured four-step exchange not only streamlines connectivity but also supports redundancy by allowing clients to select among multiple DHCP servers (Droms)



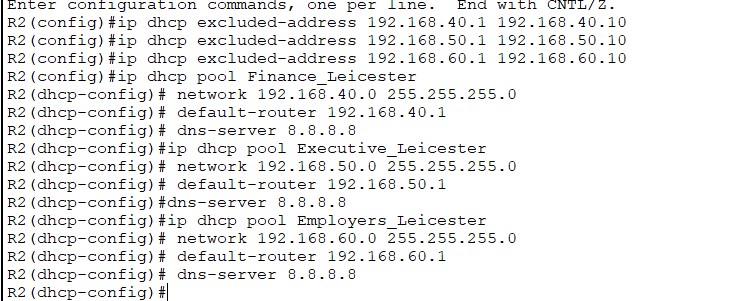
*Figure 49*



*Figure 50*



*Figure 51*

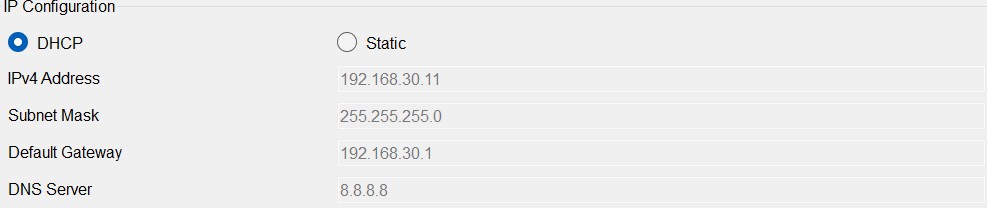


*Figure 52*

# DHCP Testing

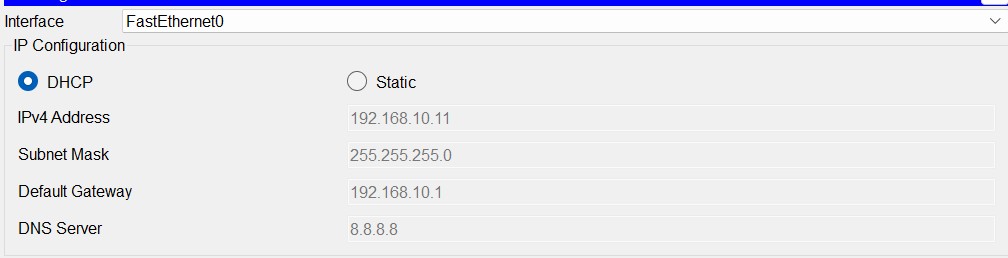
## London Area

PC -Employers



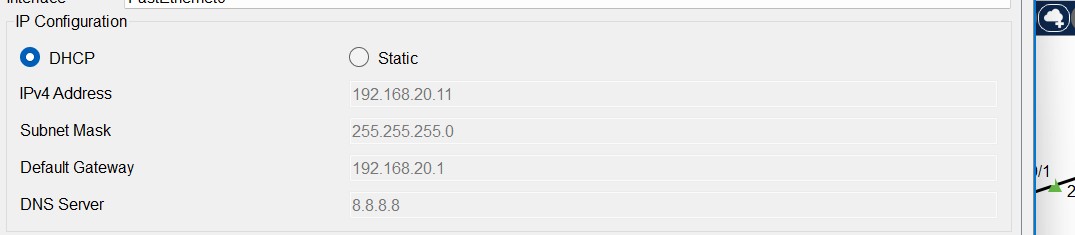
*Figure 53*

PC-Finance



*Figure 54*

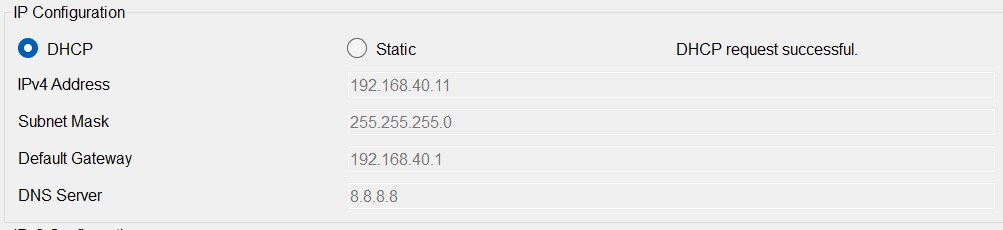
PC-Executive



*Figure 55*

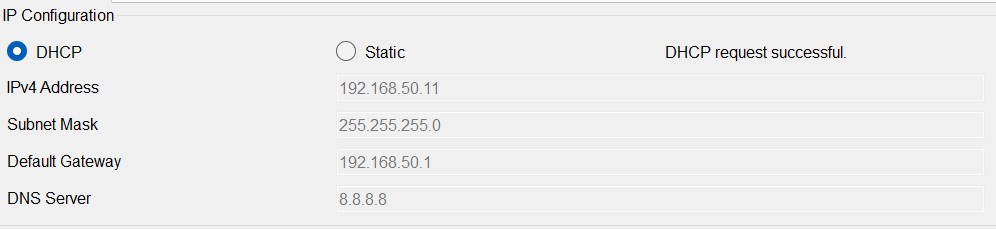
## Leicester Area

PC-Finance



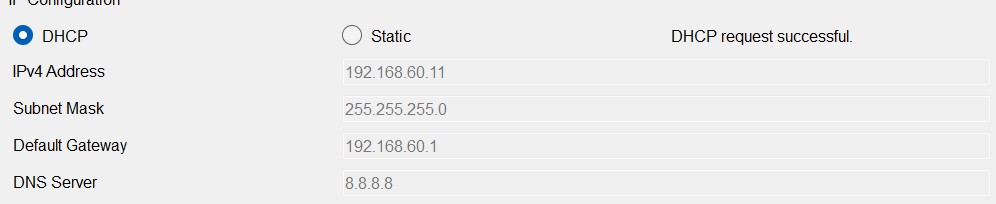
*Figure 56*

PC-Executive



*Figure 57*

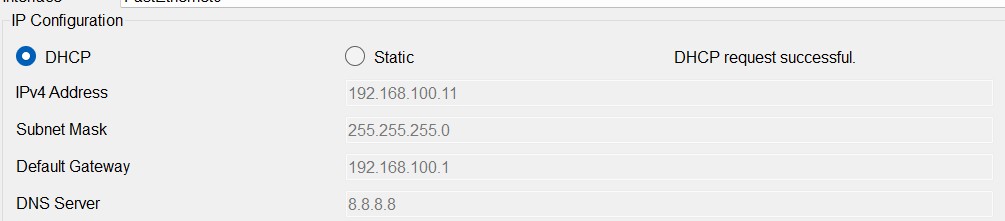
PC-Employers



*Figure 58*

## Liverpool Area

PC-Finance



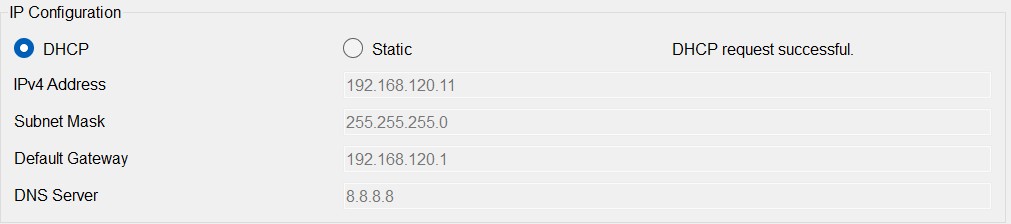
*Figure 59s*

PC-Executive



*Figure 60*

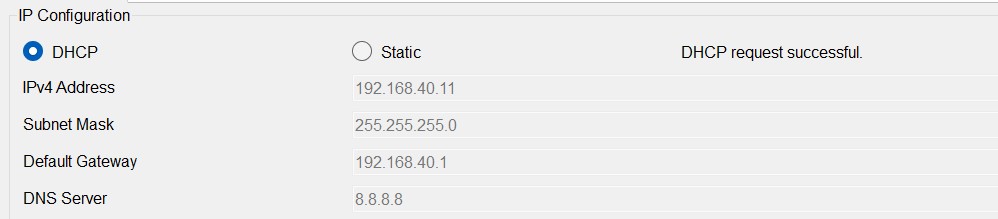
PC-Employers



*Figure 61*

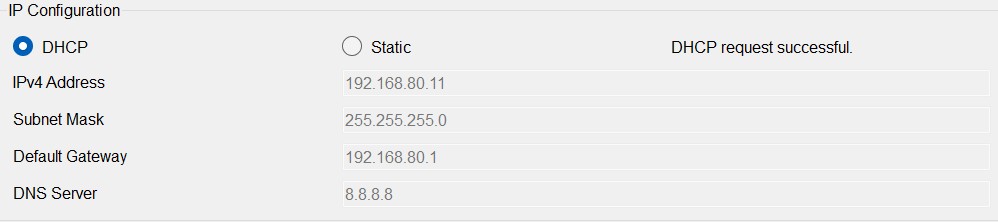
## Leeds Area

PC-Finance



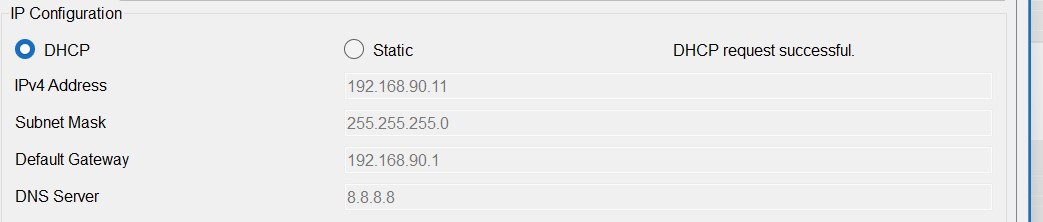
*Figure 62*

PC-Executive



*Figure 63*

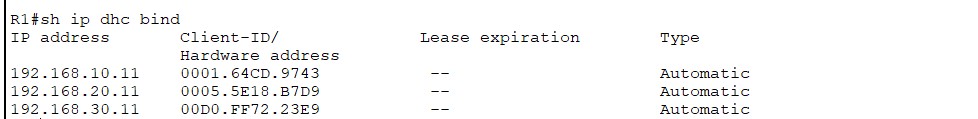
PC-Employers



*Figure 64*

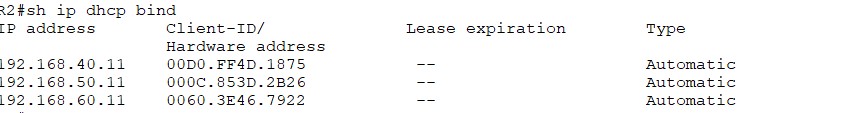
## DHCP Verification

R1 London



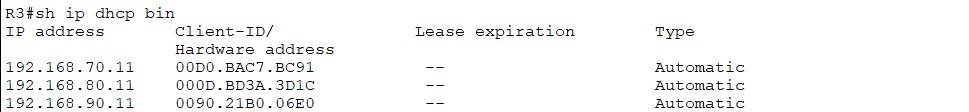
*Figure 65*

R2 Leicester



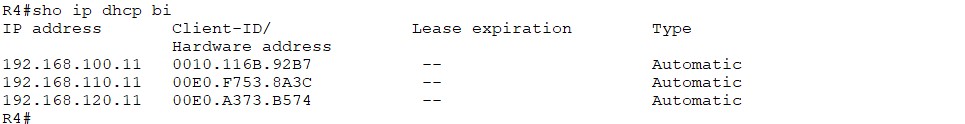
*Figure 66*

R3 Leeds



*Figure 67*

R4 Liverpool

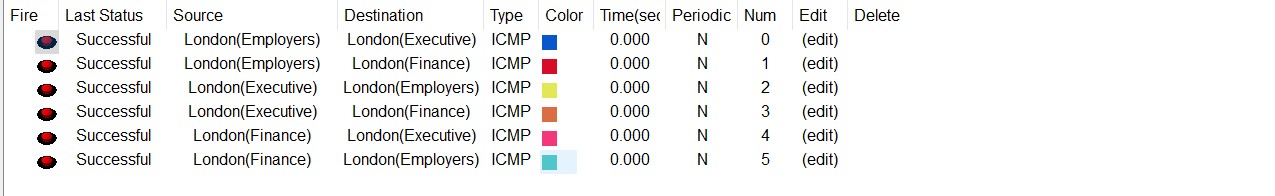


*Figure 68*

To confirm the successful allocation of IP addresses via DHCP, the show ip dhcp binding command was used on the router. This command displays a list of dynamically assigned IP addresses along with the corresponding MAC addresses of the client devices. By matching these bindings with the expected VLAN ranges and devices, it provides concrete evidence that the DHCP server is functioning correctly and assigning IPs as per the defined pools. This step ensures transparency and traceability in IP address management, reinforcing the reliability of the automated configuration process (Droms).

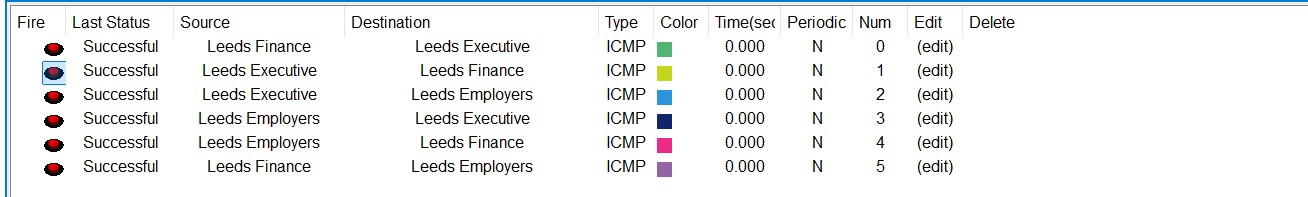
# Ping Testing

## London area



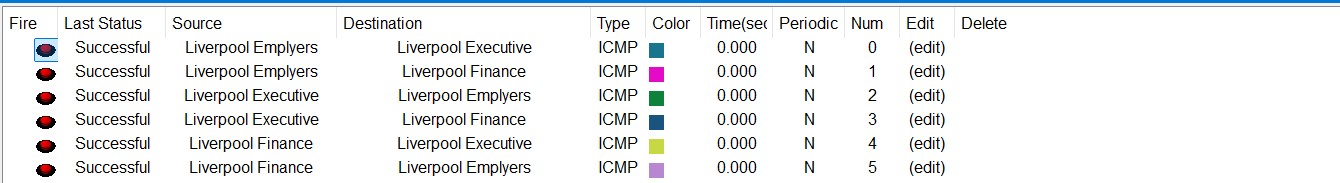
*Figure 69*

## Leeds area



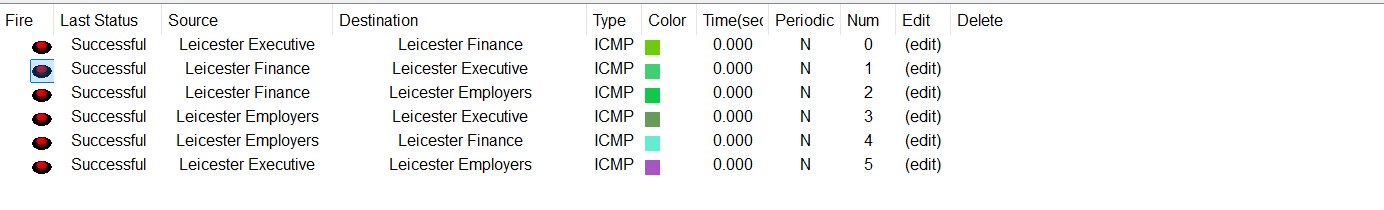
*Figure 70*

## Liverpool area



*Figure 71*

## Leicester area



*Figure 72*

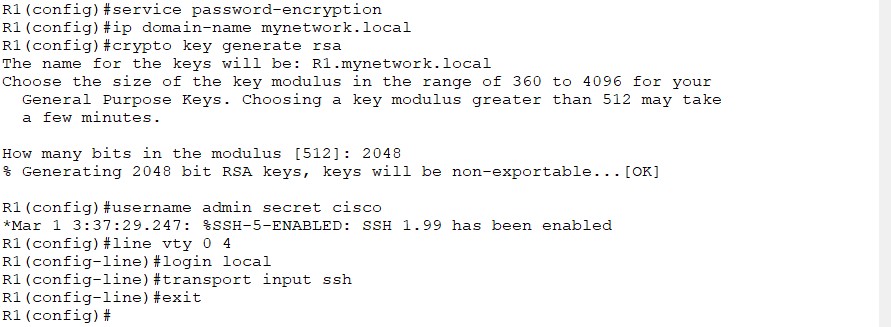
Successful ping tests were performed between devices within each region to confirm proper IP assignment and local connectivity. The 100% success rate across all sites verifies that DHCP is functioning correctly and that VLAN configurations are supporting effective intra-site communication

# Security

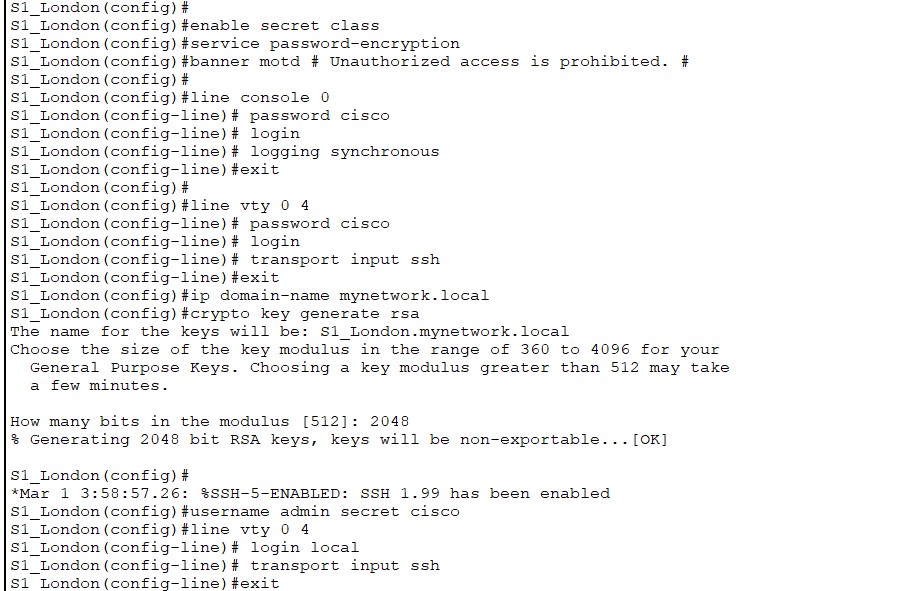
To secure the network infrastructure, essential configurations were applied to all routers and switches. Console and VTY lines were protected with passwords, and the service password-encryption command was used to prevent plain-text exposure of credentials. Insecure protocols like Telnet were disabled and replaced with SSH to ensure encrypted remote access. A login banner was also set to provide a legal warning and deter unauthorized users.

These measures align with best practices and significantly reduce risks such as unauthorized access and credential leakage. As noted by G. Mason and J. Newcomb, securing access points on network devices is crucial for maintaining overall network integrity.

## London,Router

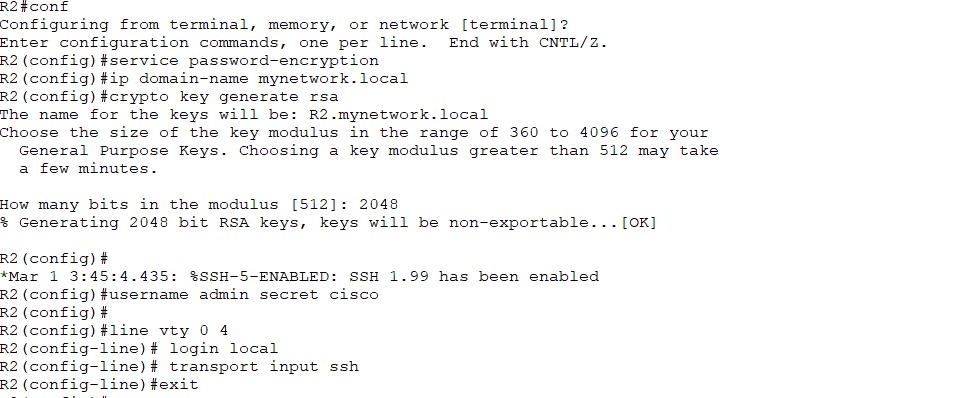


*Figure 73*

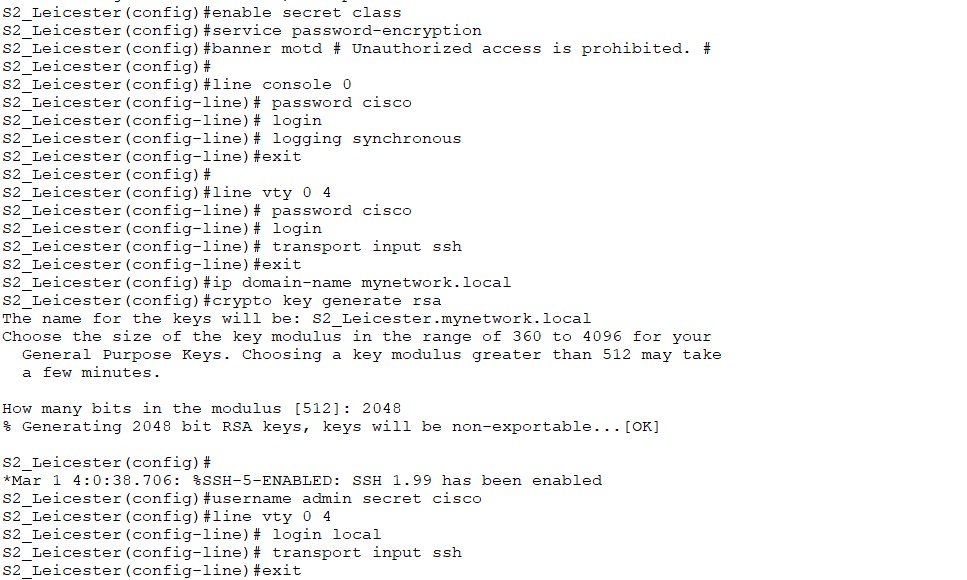


*Figure 74*

## Leicester

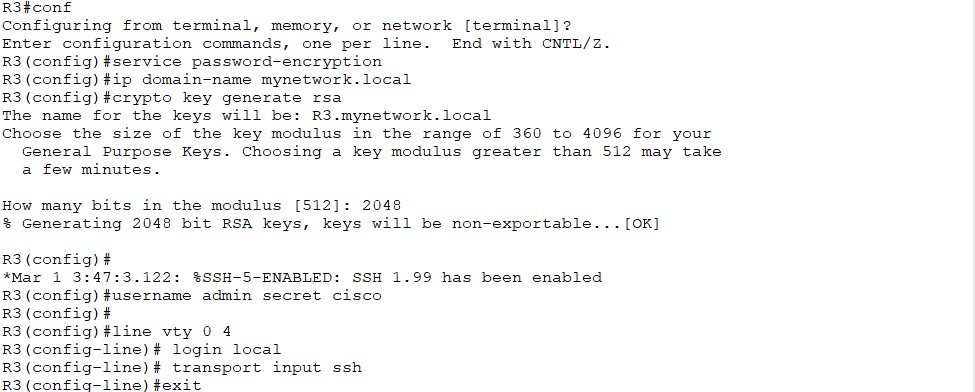


*Figure 75*



*Figure 76*

## Leeds

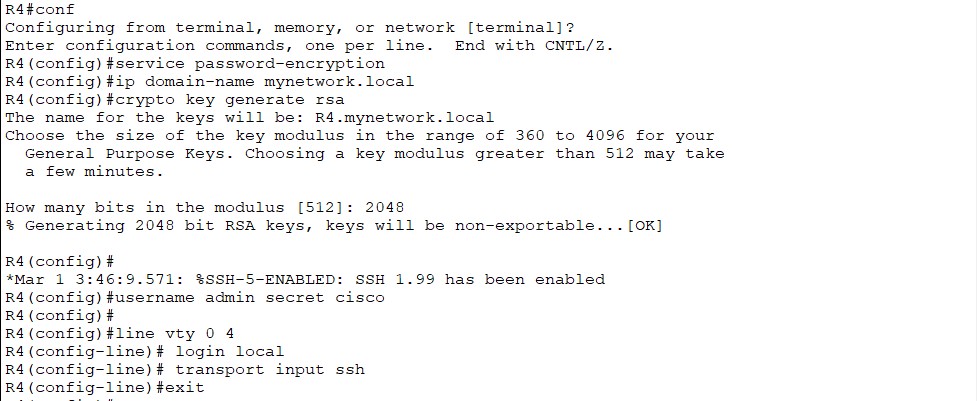


*Figure 77*

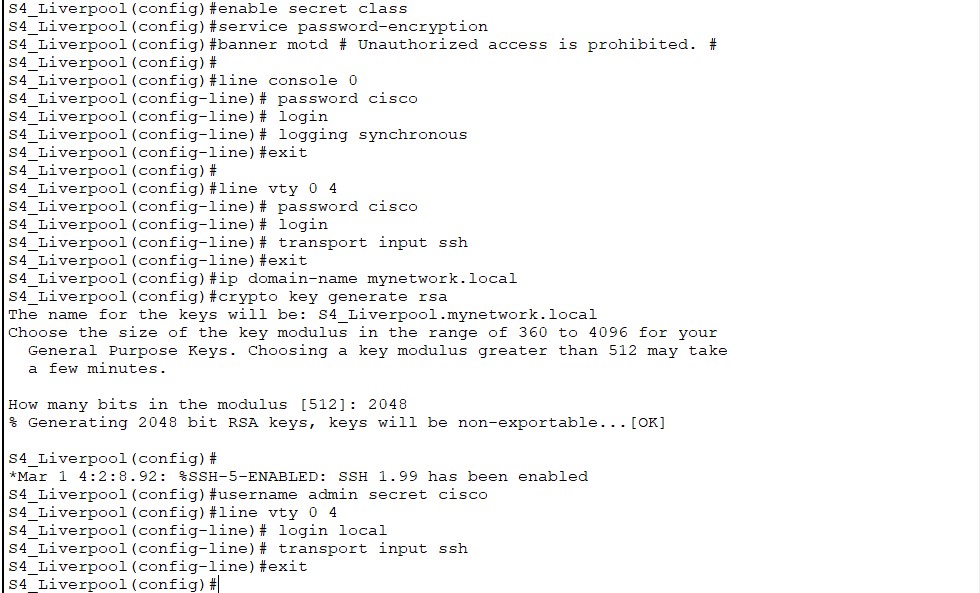


*Figure 78*

## Liverpool



*Figure 79*

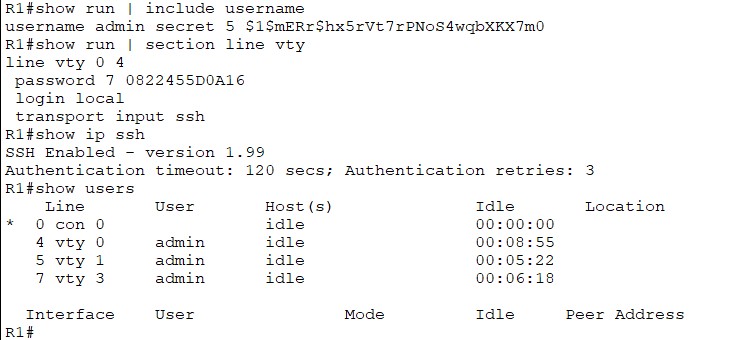


*Figure 80*

Security Verification:

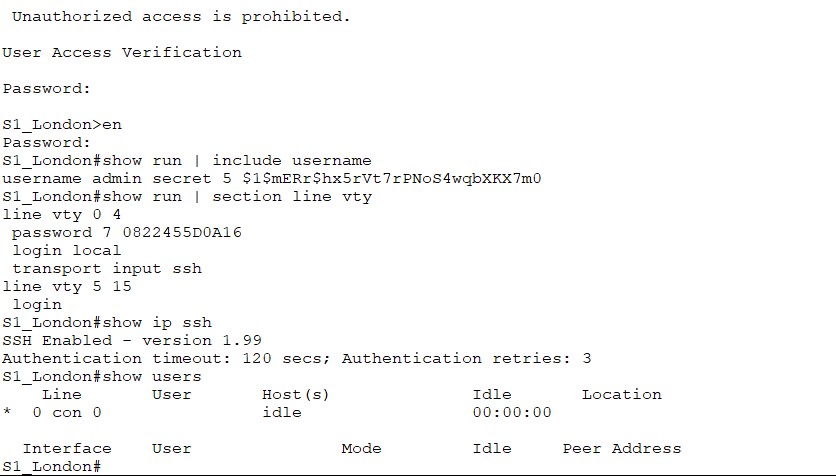
## London

Router



*Figure 81*

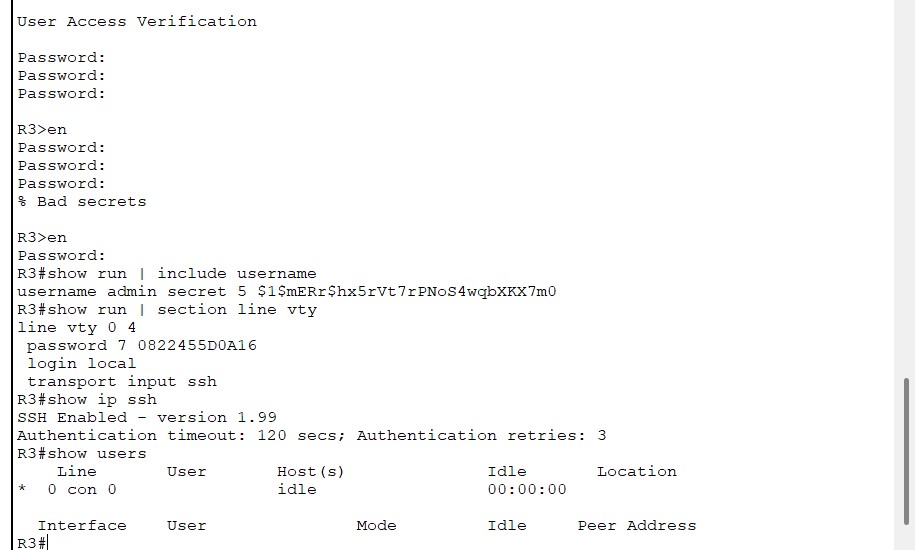
Switch



*Figure 82*

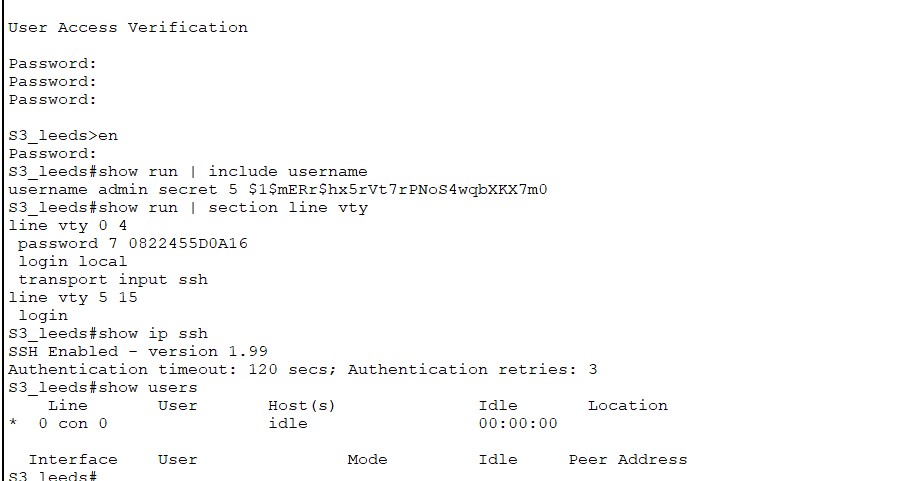
## Leeds

Router



*Figure 83*

Switch



*Figure 84*

## Liverpool

Router



*Figure 85*

Switch



*Figure 86*

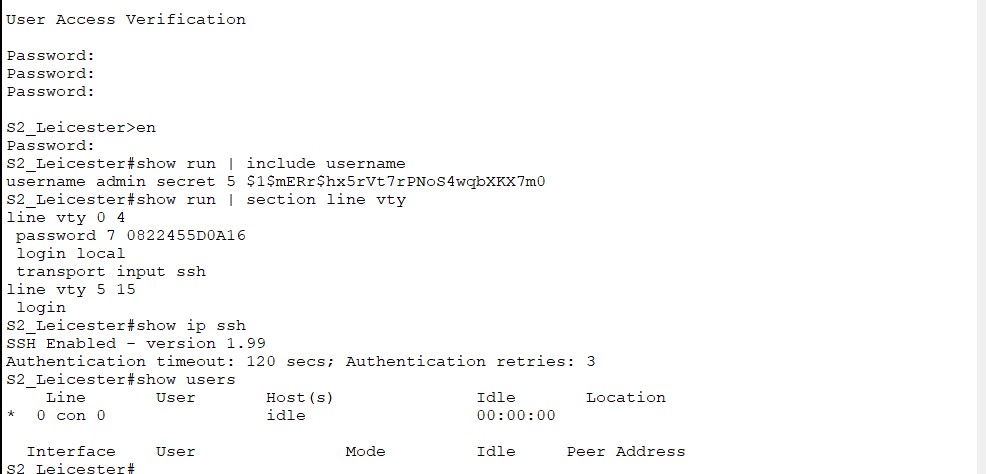
## Leicester

Router



*Figure 87*

Switch



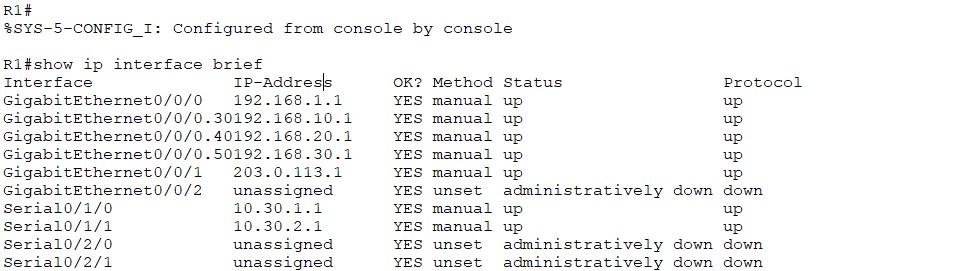
*Figure 88*

Security measures were implemented on all routers and switches to restrict unauthorized access. This included setting encrypted passwords, securing console and VTY access, enabling SSH, and disabling Telnet. A legal banner was configured, and service password-encryption was applied to protect plaintext passwords. All settings were verified using appropriate show commands and saved to the startup configuration.

# Verifying Security of Open Ports

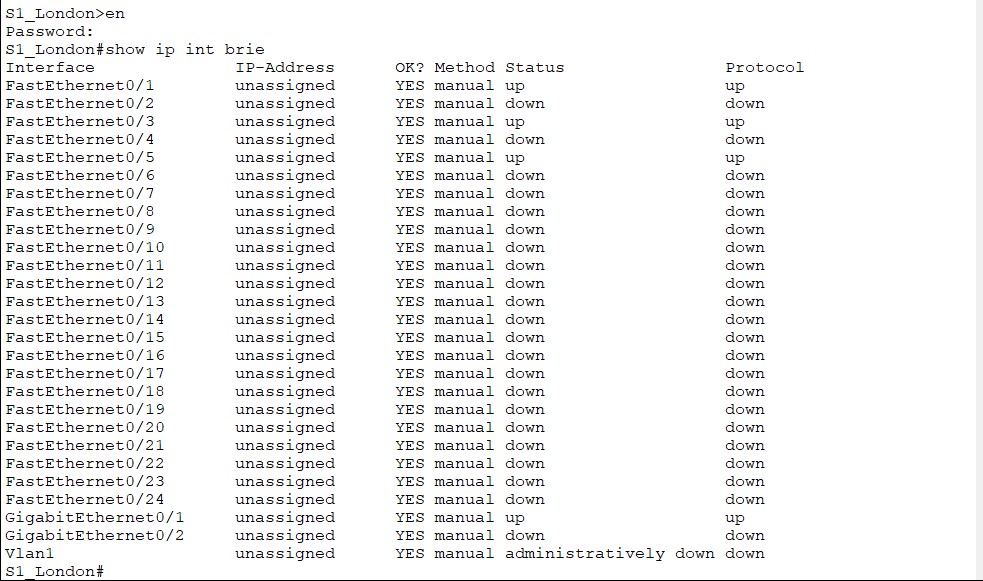
## London

Router



*Figure 89*

Switch

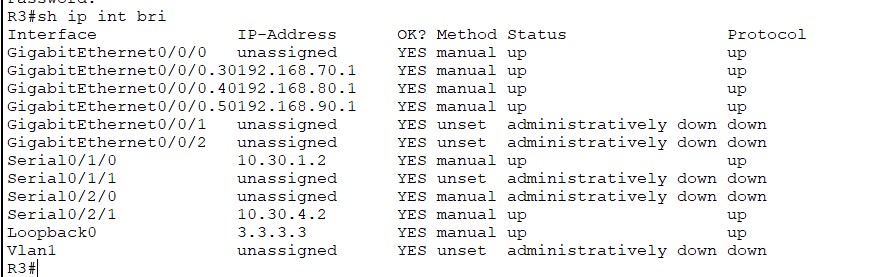


*Figure 90*

## Leeds

Router

*Figure 91*



*Figure 91*

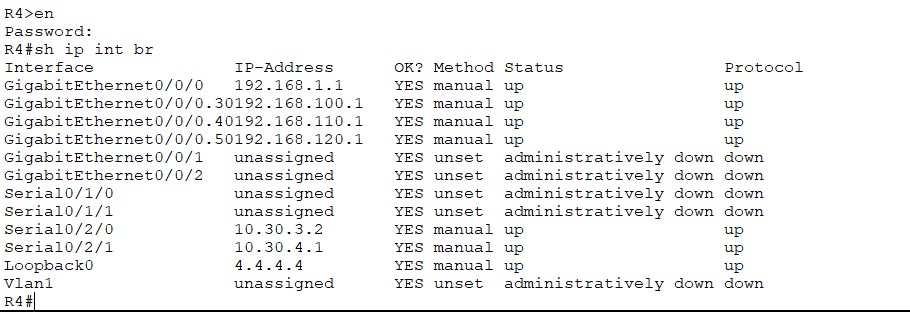
Switch



*Figure 92*

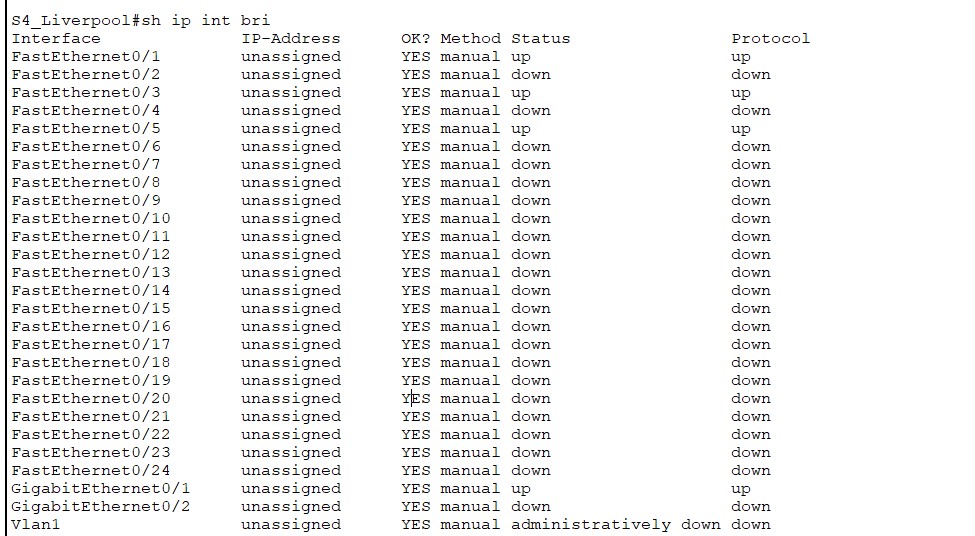
## Liverpool

Router



*Figure 93*

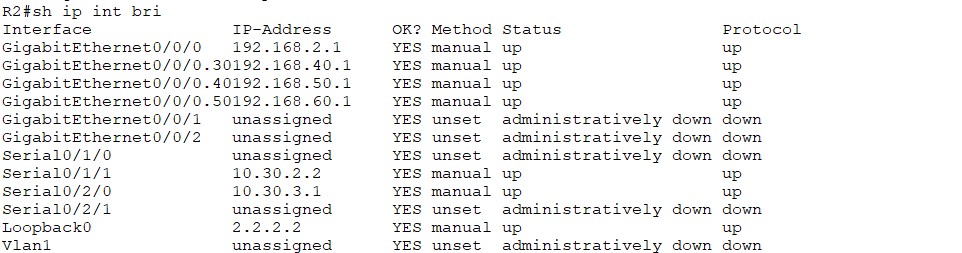
Switch



*Figure 94*

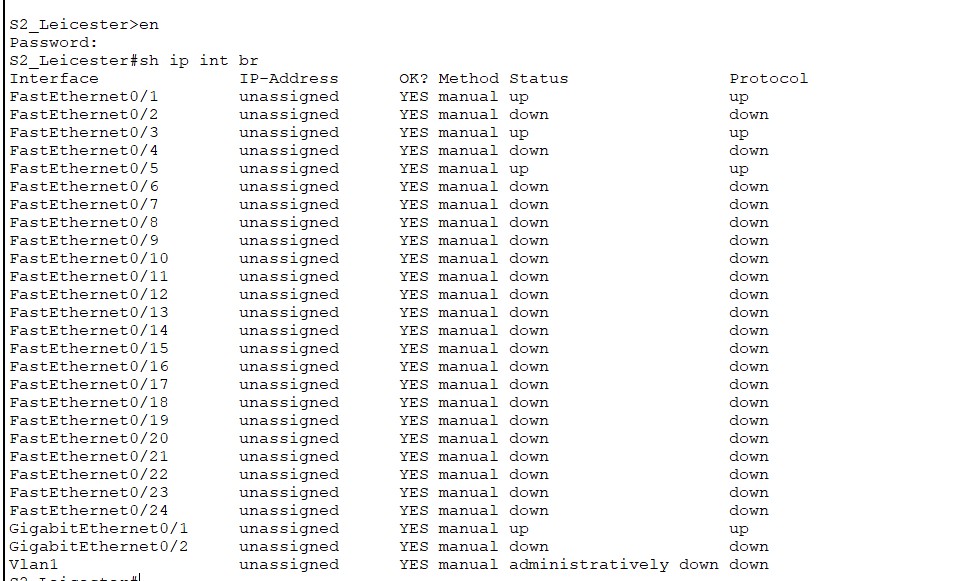
## Leicester

Router



*Figure 95*

Switch



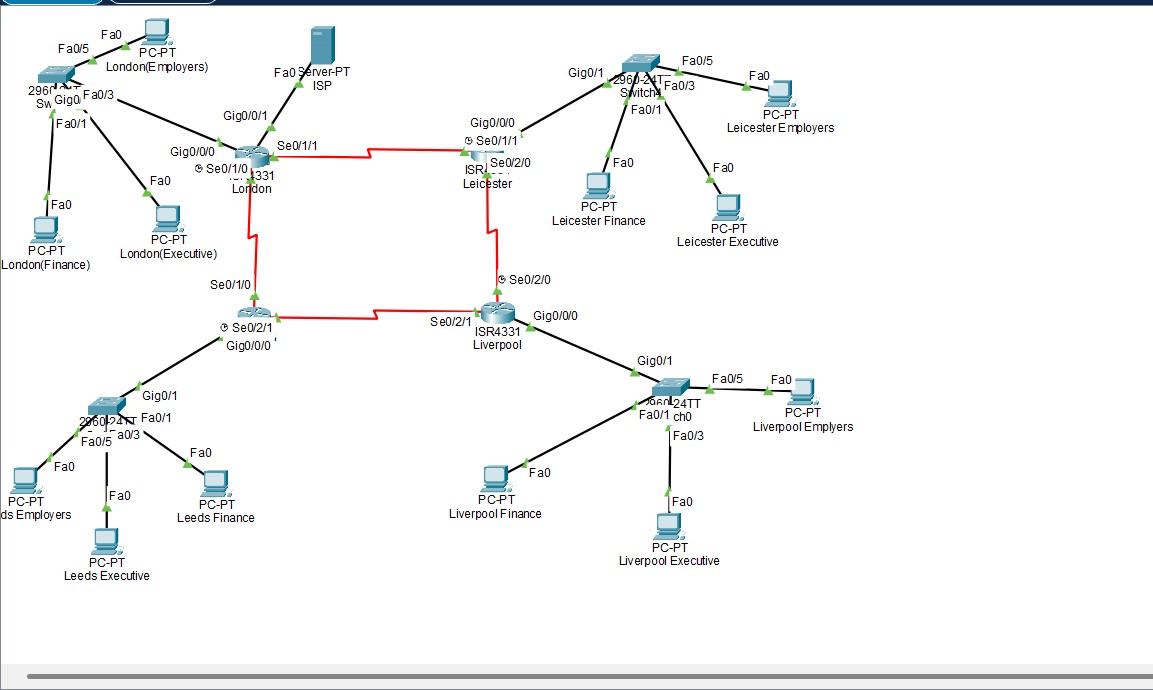
*Figure 96Figure 97*

To strengthen network security, all unused interfaces on routers and switches were administratively shut down. Leaving ports open poses a potential risk, as attackers may exploit them using techniques such as port scanning, TCP replay, or denial-of-service (DoS) attacks. As demonstrated by Al-Bahadili and Hadi (2010), proactive port control mechanisms like Hybrid Port Knocking emphasize the importance of closing unused ports to minimize attack surfaces. Even though HPK applies to advanced security setups, the principle of closing idle ports remains essential in any secure network design.

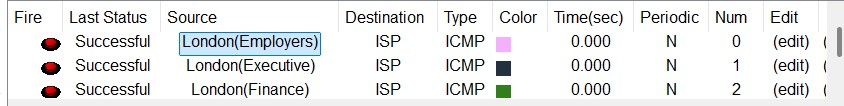
# ACL

Access Control Lists (ACLs) offer a powerful mechanism to manage and secure network traffic. In this design, ACLs were used to restrict internet access for all sites except London, enhancing security and traffic control. ACLs help network administrators regulate access by filtering packets based on IP address and protocol, restrict unauthorized communication, and improve performance by reducing unnecessary traffic. Additionally, they assist in controlling the types of traffic allowed into or out of router interfaces. However, it is important to design ACLs efficiently, as poorly constructed lists can introduce latency and impact performance across the network (Tomar & Tyagi, 2014).

Final Testing for server connection with PC before implementing ACL:



London – ISP



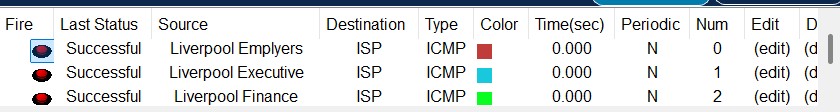
*Figure 98*

Leicester-ISP:



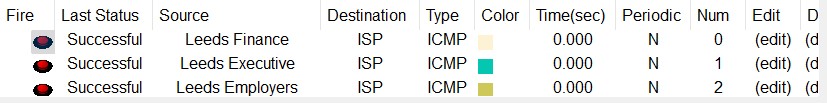
*Figure 99*

Liverpool-ISP:



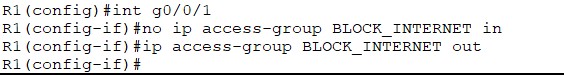
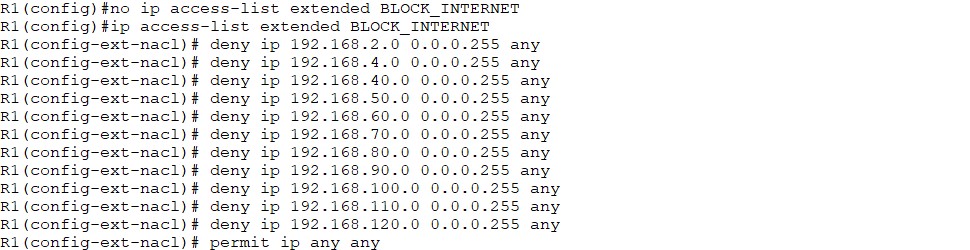
*Figure 100*

Leeds-ISP:



*Figure 101*

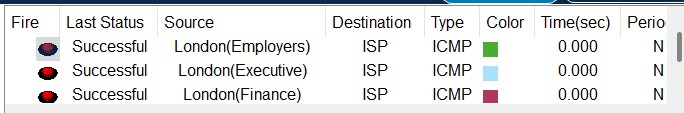
ACL implementation:



*Figure 102*

# ACL Testing

London-ISP



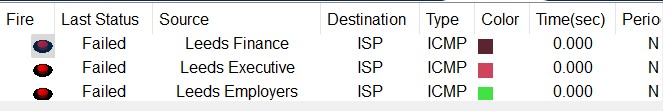
*Figure 103*

Leicester-ISP



*Figure 104*

Leeds-ISP



*Figure 105*

Liverpool-ISP



*Figure 106*

The implementation of ACLs across the network successfully enforced access restrictions, particularly preventing users in specified VLANs from reaching the ISP. Final ping tests confirmed that only permitted traffic was allowed, while unauthorized requests were blocked as intended. This configuration enhances network security, controls resource access, and ensures compliance with organizational policies

Final view

*Figure 107*

# Summary

This report detailed the end-to-end design and implementation of a secure, scalable, and resilient enterprise network interconnecting four regional sites: London, Leicester, Liverpool, and Leeds. The core of the routing architecture leveraged OSPF for dynamic path selection, with static routes serving as a reliable fallback mechanism to maintain connectivity during link failures.

The network was logically segmented using VLANs (Finance, Executive, and Employers) to enhance security and manageability, with inter-VLAN routing implemented via the router-on-a-stick method. DHCP services were configured to automate IP address assignment, ensuring operational efficiency and ease of scalability.

Access to external resources was tightly controlled using Access Control Lists (ACLs), restricting internet connectivity to the London site, while enforcing segmentation and security across all other locations. Additionally, best practices in router and switch hardening were applied, including encrypted credentials, disabled Telnet access, and shutdown of unused interfaces.

All configurations were rigorously tested through IP binding verification, inter-site and intra-VLAN connectivity tests, fallback simulations, and secure access validations. The resulting network infrastructure delivers high availability, robust security, and compliance with organizational requirements, positioning it for future growth and operational excellence.

# References

1. Aziz, Dlnya Abdulahad. “The Importance of VLANs and Trunk Links in Network Communication Areas.” International Journal of Scientific and Engineering Research, vol. 9, 2018, pp. 245–267.
2. Cisco. “Configuring VLANs.” Cisco,

www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5\_x/nxos/layer2/configuration/guide/Cisco\_Nexus\_7000\_Series\_NX-

OS\_Layer\_2\_Switching\_Configuration\_Guide\_Release\_5-x\_chapter4.html.

3 .Droms, R. “Automated Configuration of TCP/IP with DHCP.” IEEE Internet Computing, vol. 3, no. 4, 1999, pp. 45–53, https://doi.org/10.1109/4236.780960.

1. G.Mason, Andrew , and Mark J.Newcomb. “Cisco Secure Internet Security Solutions.”

Google Books,

2025,books.google.co.uk/books?hl=en&lr=&id=8D90NjKvmBAC&oi=fnd&pg=PR2&dq=s ignificance+of+security+in+cisco&ots=EWQ1wfOeJd&sig=UgZgGH9PELRT71ZfbkSTaSCFkY&redir\_esc=y#v=onepage&q=significance%20of%20security%20in%20ci sco&f=false. Accessed 14 Apr. 2025.

1. Gavin, Brady. “How to Use the Ping Command to Test Your Network.” How-to Geek, How-To Geek, 21 Aug. 2023, www.howtogeek.com/355664/how-to-use-ping-to-testyour-network/.
2. Lai, Wei Kuang, et al. “Dynamic Appointment of ABR for the OSPF Routing Protocol.” Computer Communications, vol. 31, no. 14, Sept. 2008, pp. 3098–3102, https://doi.org/10.1016/j.comcom.2008.04.011. Accessed 24 May 2022.
3. Medhi, Deep, and Karthik Ramasamy. “Routing Algorithms: Shortest Path, Widest Path, and Spanning Tree.” Network Routing, 2018, pp. 30–63, https://doi.org/10.1016/b978-012-800737-2.00003-x. Accessed 7 Oct. 2024.
4. Sun, Xin, et al. “A Systematic Approach for Evolving VLAN Designs.” IEEE Xplore, 1 Mar.

2010, ieeexplore.ieee.org/abstract/document/5461961/.

1. Al-Bahadili, H. and Hadi, A.H., 2010. Network security using hybrid port knocking. Ijcsns, 10(8), p.8.