2024

Basic Network Design for a business company or an organisation

LOK WING LAVIN WONG
[21386055]

Contents

Abstract

This network design report presents the thorough planning and execution of a strong networking infrastructure for a company. The main objective was to provide accommodations for 40 hosts in two offices in each of the two locations—Manchester and London. To effectively manage IP addresses for networking devices, a CIDR IP addressing scheme was used. Specifications for configuring networking devices are given, along with screenshots of the devices. The report displays connectivity tests between PCs in various offices to prove smooth communication. Security precaution configurations for remote router management were used. The report likewise emphasises the effective deployment and validation of DHCP and RIP configurations as necessary. This study provided an overview of the network architecture, including element configurations and a network evaluation of the design. With regard to optimum performance, security, and scalability, this network architecture seeks to satisfy the needs of the company.

Introduction

As a network engineer assigned to build a solid network infrastructure for a new business with two locations (Manchester and London), this report describes the detailed network design proposal that was created using Cisco Packet Tracer as a simulation tool. Connectivity tests between PCs in different offices, setting up a secure password and Secure Shell (SSH) access on one of the routers for remote management, and demonstrating and validating the implementation of Routing Information Protocol (RIP) and Dynamic Host Configuration Protocol (DHCP) were among the requirements that the network design is essential to meet.

In order to methodically accomplish these tasks, this report is divided into different sections, each of which concentrates on an essential component of the network configuration. The content will cover the complete network design and configurations, router and PC configuration, and connectivity between different offices. It will also demonstrate how security precautions are implemented and verified, such as passwords and secure shells (SSH) as remote management functions, and how RIP and DHCP configurations work flawlessly.

Aim and Objectives

The aim is to design a network for a business or an organisation. The objectives are:

1. to create a medium-sized network with wired and wireless access that can accommodate 40 hosts (PCs) spread across two offices at each location;
2. to implement a CIDR addressing;
3. to configure passwords for router remote management;
4. to configure SSH to secure a remote access login on routers;
5. to configure network devices;
6. to do connectivity tests between PCs in different offices;
7. to verify RIP and DHCP configurations appropriately;
8. to show a complete connected network design;
9. deliver tips or recommendations for designing an optimised network at the end of this report.

Network Design

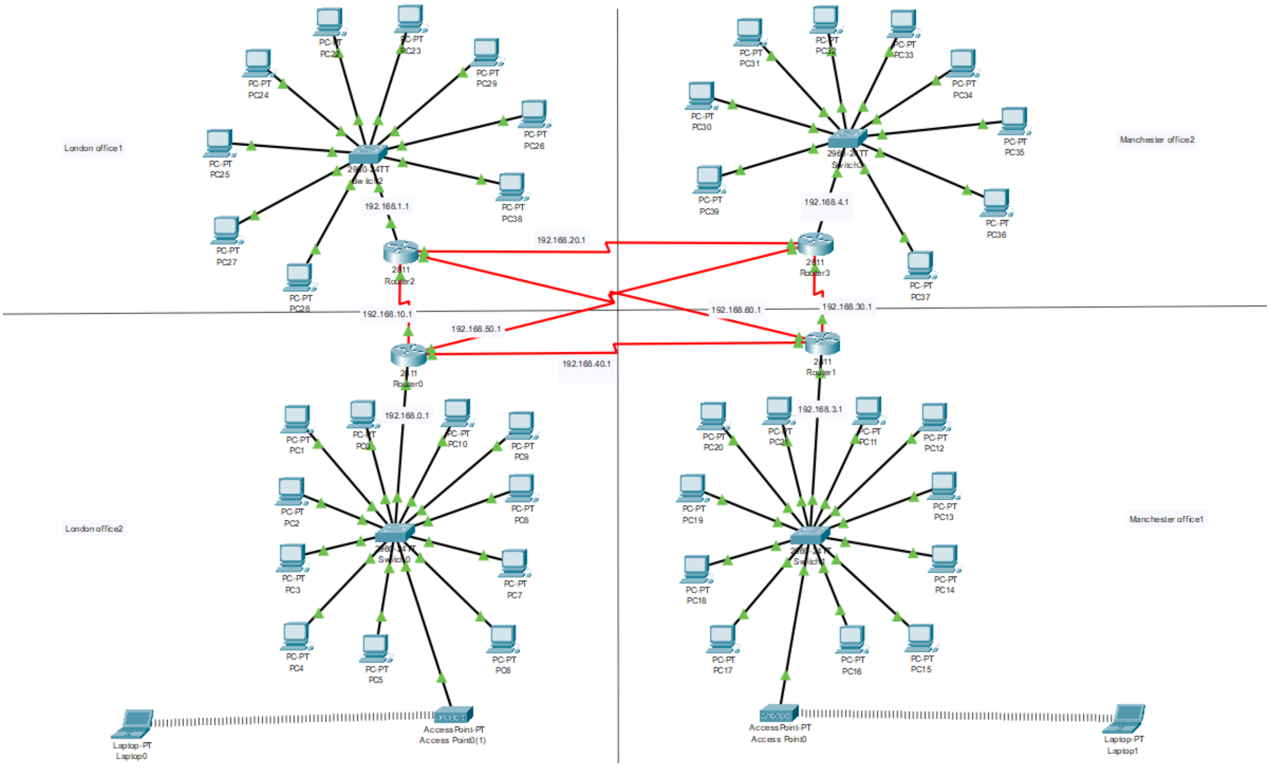


Figure 1: Complete network design

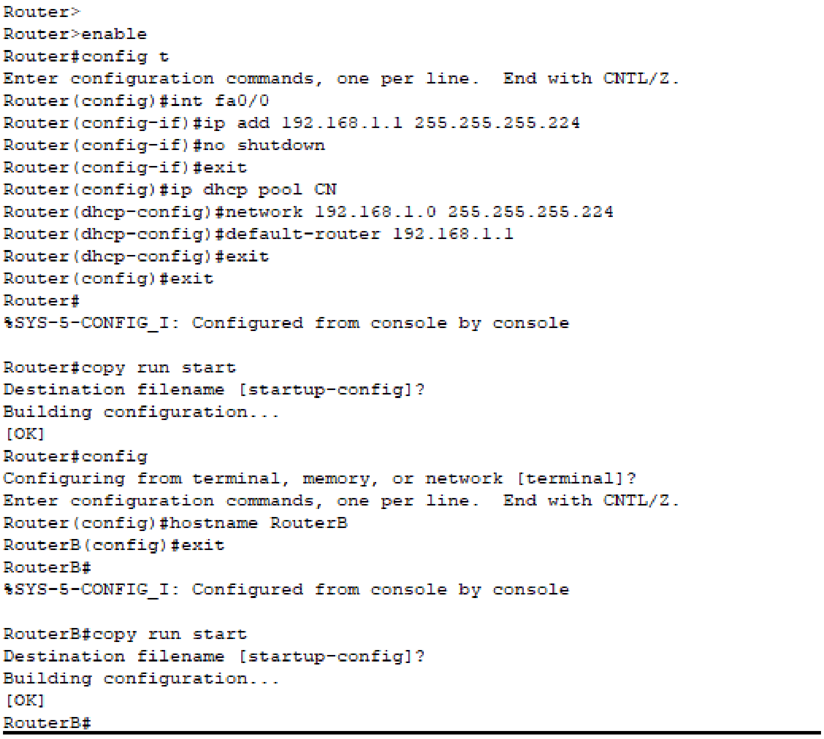
Network Plan

The network design for the dual offices in London and Manchester, respectively, reflects a comprehensive strategy to establish a robust, secure, and scalable infrastructure. With the organisation's unique requirements in mind, this painstaking plan was created to give connectivity, performance, and security first priority. The network's body is made up of four routers that are thoughtfully arranged in each office and connected by serial DCEs (Data Circuit-terminating Equipment). Since Serial DCE is excellent at long-distance connections and offers dependable and effective point-to-point connectivity between geographically separated offices, the decision to utilising it was carefully planned out.

Within each office, the deployment of switches facilitated connectivity within the local network. Copper Straight-Through cables were chosen because of their ease of use and efficiency in local network settings for connecting switches to routers and routers to end-user devices. Compatibility and simplicity of use in a local area network (LAN) environment are guaranteed by this standard connection type. The network design is flexible enough to accommodate both wired and wireless end-user devices, as demonstrated by the use of Copper Straight-Through cables for PCs and wireless connectivity through access points.

Network Configuration

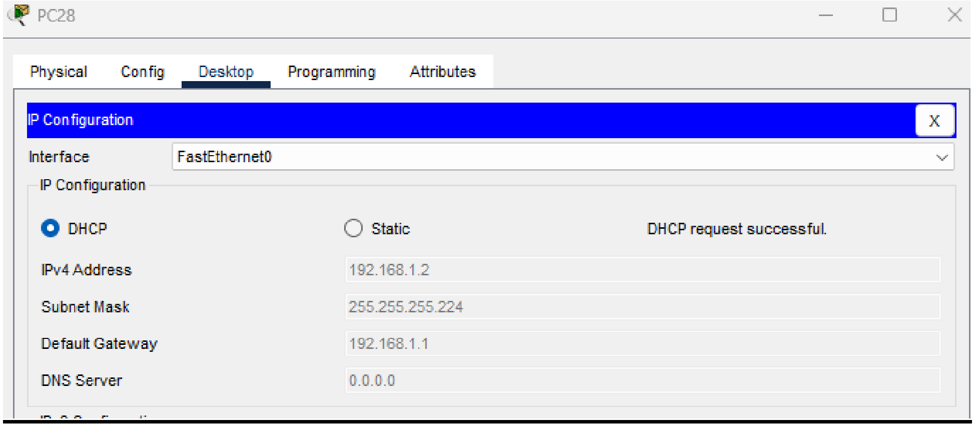
The network setup has been carefully configured to guarantee dynamic routing between the Manchester and London offices, effective IP address management, and security. To create a reliable and effective network infrastructure, the essential components consist of router passwords, Routing Information Protocol (RIP), Secure Shell (SSH), and Dynamic Host Configuration Protocol (DHCP). They were meticulously established in position as below:



```
Router>
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.224
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip dhcp pool CN
Router(dhcp-config)#network 192.168.1.0 255.255.255.224
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterB
RouterB(config)#exit
RouterB#
%SYS-5-CONFIG_I: Configured from console by console

RouterB#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
RouterB#
```

Figure 2: DHCP configuration

- **Dynamic Host Configuration Protocol (DHCP)**:
  DHCP is a protocol that provides automatic IP address assignment and configuration information to each host in the network, making IP address administration more efficient and convenient (Yoo and Kim, 2016). The implementation of it reduces the requirement for manual assignment and simplifies the IP address management procedure in the design. By minimising human mistakes and increasing efficiency, DHCP makes sure that devices may connect to the network automatically without the need for human interaction. This makes network administration easier overall, which is especially useful in settings with lots of devices.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.224

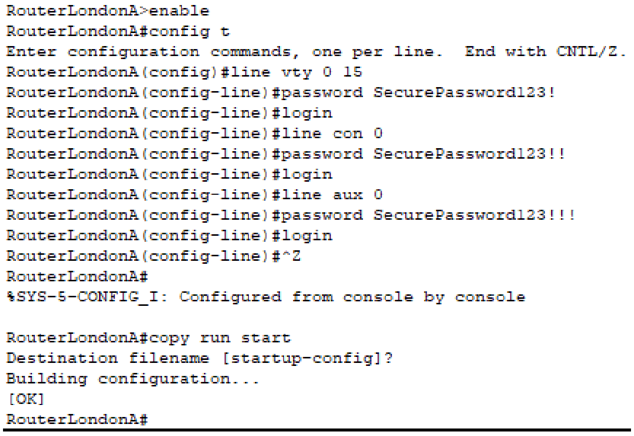
Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

Figure 3: IP configuration on a PC

- **IP addressing**:

  In terms of IP addressing, the adoption of the CIDR (Classless Inter-Domain Routing) scheme was instrumental in efficiently allocating IP addresses and implementing subnetting for network optimization. CIDR's flexibility allows for the dynamic assignment of IP addresses and facilitates subnetting, resulting in a more efficient use of IP address space. Subnetting, in turn, organises network addresses logically, enhancing security and simplifying troubleshooting by localising issues within specific subnets. This approach not only accommodates the current network requirements but also positions the organisation for future growth and scalability.

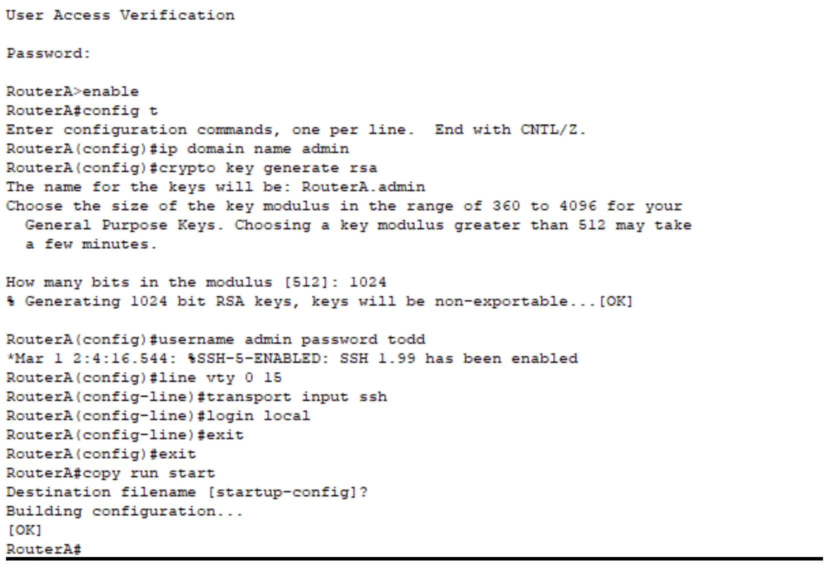


```
RouterLondonA>enable
RouterLondonA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterLondonA(config)#line vty 0 15
RouterLondonA(config-line)#password SecurePassword123!
RouterLondonA(config-line)#login
RouterLondonA(config-line)#line con 0
RouterLondonA(config-line)#password SecurePassword123!!
RouterLondonA(config-line)#login
RouterLondonA(config-line)#line aux 0
RouterLondonA(config-line)#password SecurePassword123!!!
RouterLondonA(config-line)#login
RouterLondonA(config-line)#^Z
RouterLondonA#
%SYS-5-CONFIG_I: Configured from console by console

RouterLondonA#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
RouterLondonA#
```

Figure 4: Password set up on a router

- **Router Passwords**:

  A router is a network communication device that connects different networks and efficiently passes data packets on a network to their next location, and password authentication is used for access control and router administration; hackers could be able to crack it and access the router and the network if the password is weak and insecure (Farik and Ali, 2015). Router passwords must be configured as part of the configuration to improve network security. As a vital first layer of defence, passwords prevent unauthorised users from accessing router configurations. This essential security feature guarantees that only authorised individuals may modify the router settings, protecting confidential network data.

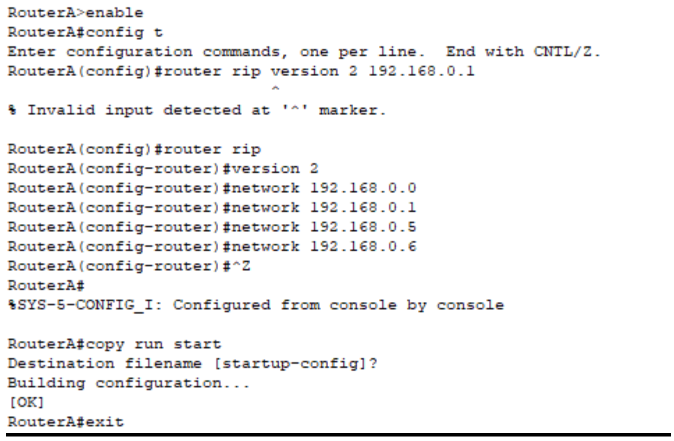


```
User Access Verification

Password:

RouterA>enable
RouterA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)#ip domain name admin
RouterA(config)#crypto key generate rsa
The name for the keys will be: RouterA.admin
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]

RouterA(config)#username admin password todd
*Mar 1 2:4:16.544: %SSH-5-ENABLED: SSH 1.99 has been enabled
RouterA(config)#line vty 0 15
RouterA(config-line)#transport input ssh
RouterA(config-line)#login local
RouterA(config-line)#exit
RouterA(config)#exit
RouterA#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
RouterA#
```

Figure 5: SSH configuration

- **Secure Shell (SSH)**:

  Secure Shell is an application that allows you to transfer files between computers, log into another computer via a network, and run commands on a distant computer. It is a cryptographic network protocol used to provide a secure method for remotely accessing and managing network devices (Garimella and Kumar, 2015). Unlike less secure options like Telnet, SSH encrypts the user-to-router connection to shield against illegal interception or possible eavesdropping. According to current security best practices, this guarantees a private and secure path for remote management in the company.



```
RouterA>enable
RouterA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)#router rip version 2 192.168.0.1
                           ^
% Invalid input detected at '^' marker.

RouterA(config)#router rip
RouterA(config-router)#version 2
RouterA(config-router)#network 192.168.0.0
RouterA(config-router)#network 192.168.0.1
RouterA(config-router)#network 192.168.0.5
RouterA(config-router)#network 192.168.0.6
RouterA(config-router)#^Z
RouterA#
%SYS-5-CONFIG_I: Configured from console by console

RouterA#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
RouterA#exit
```

Figure 6: RIP configuration

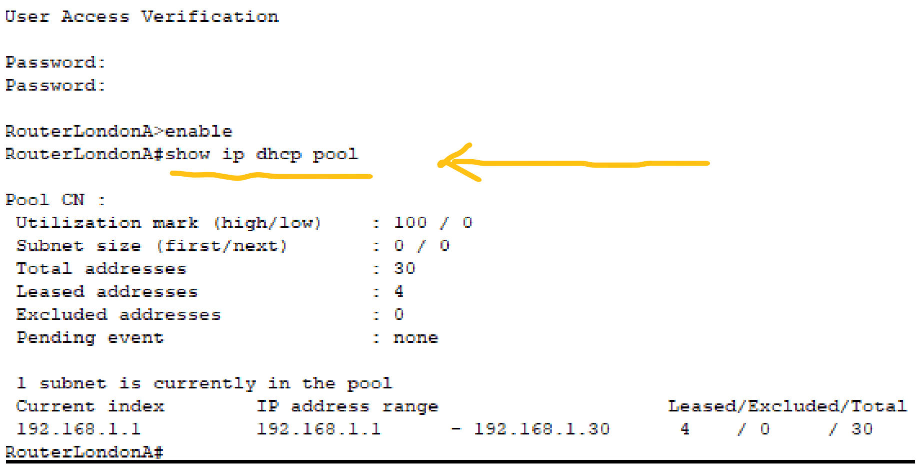
- **Routing Information Protocol (RIP)**:

  RIP is a type of vector-distance routing protocol that is commonly utilised in most networks since it uses an easy-to-implement algorithm (Yang and Yong, 2012). This tool was selected as it can facilitate dynamic routing between routers. It determines the optimal path from the source to the destination using the number hop count (distance) as a metric (Atefi et al, 2016). It exchanges routing information between routers, allowing for automatic updates of network changes (Biradar, 2020). The decision to use RIP was based on its straightforward implementation and suitability for the scale of the network. The periodic updates and route metric calculations provided by RIP contribute to efficient routing within the organisation.

To summarise, every configuration element was selected with a particular objective in mind, conforming to industry best practices and the demands of the network. A dependable and optimally optimised network infrastructure is emphasised by the focus on security, effective IP address management, and dynamic routing.

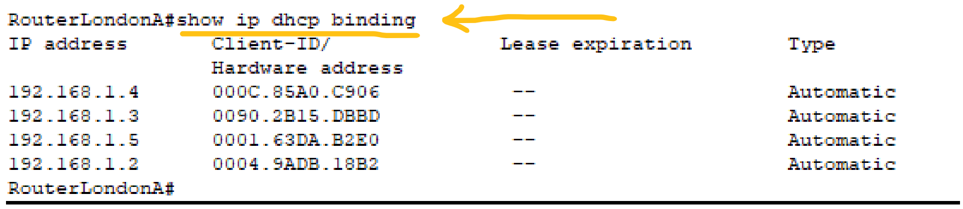
Network Verification/Configuration Test

DHCP



```
User Access Verification

Password:
Password:

RouterLondonA>enable
RouterLondonA#show ip dhcp pool

Pool CN :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 30
 Leased addresses               : 4
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.30      4     / 0     / 30
RouterLondonA#
```

Figure 7.1: Verify DHCP pool configuration

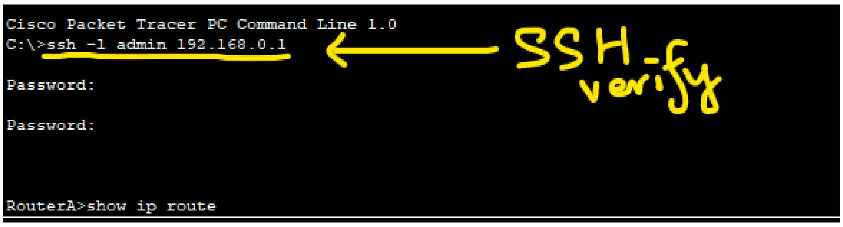


```
RouterLondonA#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.4      000C.85A0.C906           --                     Automatic
192.168.1.3      0090.2B15.DBBD           --                     Automatic
192.168.1.5      0001.63DA.B2E0           --                     Automatic
192.168.1.2      0004.9ADB.18B2           --                     Automatic
RouterLondonA#
```

Figure 7.2: Verify DHCP binding

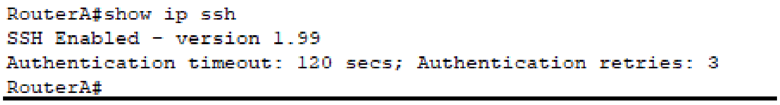
To verify the DHCP configuration, it is essential to confirm the DHCP pool configuration (Figure 6). Likewise, making sure that IP address ranges, subnet masks, default gateways, and DNS server settings, according to Figure 2, are accurate and crucial steps. To ensure that IP addresses are effectively given to clients, it is also necessary to examine DHCP bindings, as shown in Figure 7, which involves checking MAC addresses, matching issued IP addresses, and lease expiration dates. Collectively, these two crucial verification elements help to guarantee the network's smooth dynamic IP address distribution, as well as ensuring the DHCP infrastructure's dependability and effectiveness.

SSH



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.0.1

Password:

Password:


RouterA>show ip route
```

Figure 8.1: SSH verification

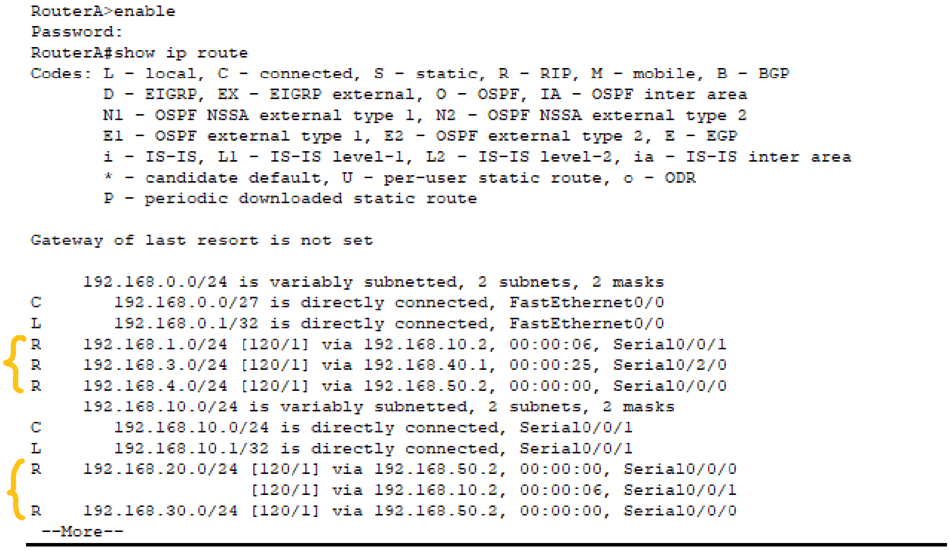


```
RouterA#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
RouterA#
```

Figure 8.2: SSH verification

A secure shell client as a PC was used to establish an SSH connection to the router that has verified SSH by looking up the SSH parameters in the running configuration (Figure 8.1). As shown in Figure 8.1, after entering the command with the router IP address correctly, the successful completion of the login process implies that the network connectivity, credentials, and SSH configuration are all in order. This accomplishment validates that the supplied username and IP address may be used to remotely access the device via SSH, guaranteeing safe and verified access to the router. In addition, it was also checked that SSH is enabled and that the SSH version has been configured as version 2 (Figure 8.2). Secure remote access is made possible by the comprehensive verification processes, which ensure the router's SSH configuration is accurate.

RIP

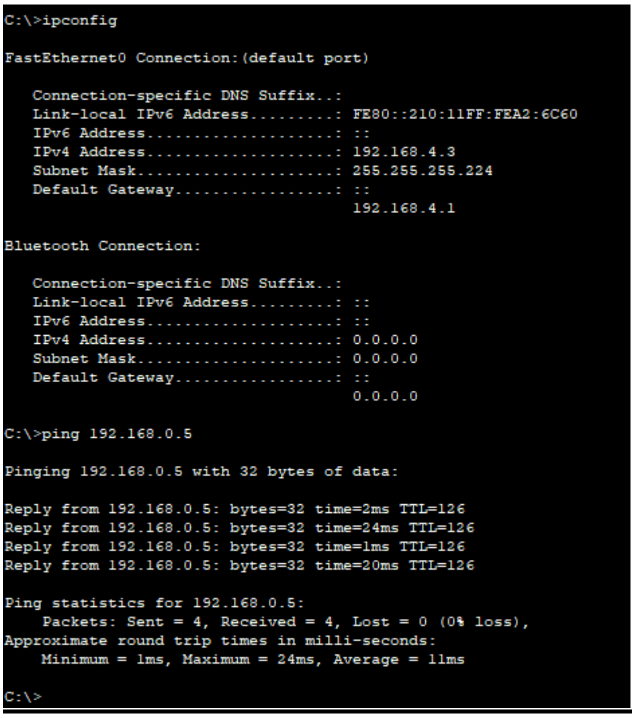


```
RouterA>enable
Password:
RouterA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/27 is directly connected, FastEthernet0/0
L       192.168.0.1/32 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/1] via 192.168.10.2, 00:00:06, Serial0/0/1
R    192.168.3.0/24 [120/1] via 192.168.40.1, 00:00:25, Serial0/2/0
R    192.168.4.0/24 [120/1] via 192.168.50.2, 00:00:00, Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, Serial0/0/1
L       192.168.10.1/32 is directly connected, Serial0/0/1
R    192.168.20.0/24 [120/1] via 192.168.50.2, 00:00:00, Serial0/0/0
                     [120/1] via 192.168.10.2, 00:00:06, Serial0/0/1
R    192.168.30.0/24 [120/1] via 192.168.50.2, 00:00:00, Serial0/0/0
 --More--
```

Figure 9: RIP verification

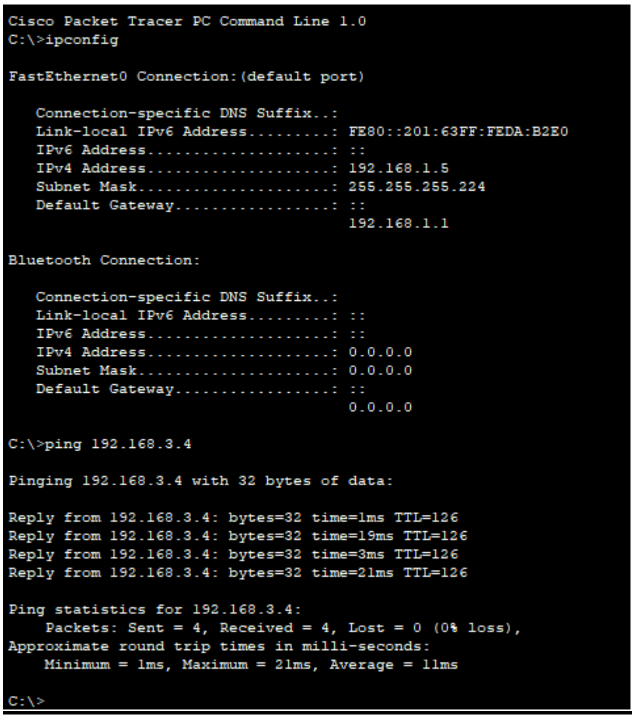
The "show ip route" command is essential for verifying a router's RIP configuration. The router's routing table is fully displayed, displaying the routes that the RIP has shown after using the command. According to Figure 9, specifically focusing on entries marked with the letter "R" in the routing table, these entries represent RIP routes, indicating that the router has received routing information from neighbouring routers using RIP. This verification ensures that the router has developed and is aware of the available network paths, facilitating optimal routing decisions and contributing to the overall stability of the network.

Verify IP addressing and Connectivity between devices



```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::210:11FF:FEA2:6C60
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.4.3
   Subnet Mask.....................: 255.255.255.224
   Default Gateway.................: ::
                                     192.168.4.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 192.168.0.5

Pinging 192.168.0.5 with 32 bytes of data:

Reply from 192.168.0.5: bytes=32 time=2ms TTL=126
Reply from 192.168.0.5: bytes=32 time=24ms TTL=126
Reply from 192.168.0.5: bytes=32 time=1ms TTL=126
Reply from 192.168.0.5: bytes=32 time=20ms TTL=126

Ping statistics for 192.168.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 24ms, Average = 11ms

C:\>
```

Figure 10: Pinging from a PC to a router in different offices



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:63FF:FEDA:B2E0
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.5
   Subnet Mask.....................: 255.255.255.224
   Default Gateway.................: ::
                                     192.168.1.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=1ms TTL=126
Reply from 192.168.3.4: bytes=32 time=19ms TTL=126
Reply from 192.168.3.4: bytes=32 time=3ms TTL=126
Reply from 192.168.3.4: bytes=32 time=21ms TTL=126

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 11ms

C:\>
```

Figure 11: ***Pinging from a PC to another PC in different offices***

Using the Ping utility to verify device connectivity is a basic and useful technique for troubleshooting networks. A successful ping verifies end-to-end connections and shows that there are no barriers preventing the devices from exchanging data packets. Additionally, network performance can be understood from the round-trip time and packet loss data that ping results provide. Robust connectivity is indicated by short round-trip times and no packet loss, but anomalies in these measures may point to network problems that need more research. For network administrators, Ping is an invaluable tool that makes it easy to quickly and accurately assess the reachability of devices and the general health of the network.

Network Evaluation and Discussion

The network design of this report carefully considers the goals of building a scalable, secure, and reliable infrastructure for a business that has offices in Manchester and London. It is crucial for us as network engineers to assess the design's rigour, scalability, redundancy, and cost implications.

Rigour:

The design demonstrates a high level of rigour by utilising a CIDR IP addressing scheme for efficient IP address management. In the process of network administration, human error is reduced due to the DHCP configuration. Robust security features like strong router passwords and SSH for remote management help to prevent unwanted access, while the addition of RIP for dynamic routing improves the network's adaptability to changes.

Scalability:

Scalability is evident in the adoption of CIDR, which allows dynamic assignment of IP addresses and facilitates subnetting. This arranges network addresses in a logical manner and sets up the company for expansion. The network's size is taken into consideration while selecting RIP, which offers a simple implementation that facilitates automatic updates in response to changes in the network. Scalability is ensured by the modular design, which allows for the addition of devices without sacrificing performance. Switches provide local connectivity.

Redundancy:

While not explicitly mentioned, the use of RIP for dynamic routing implies the network's adaptability to changes, including potential link failures. Likewise, employing a protocol like OSPF that has built-in redundancy capabilities or creating redundant links between routers should be taken into account for increased redundancy. This would improve network dependability by providing backup routes in the event of a link breakdown.

Cost Implications:

The network's scalability and security requirements are balanced with related costs in the design. Using industry-standard protocols like RIP and DHCP guarantees effectiveness without incurring extra costs. Nonetheless, a more thorough cost analysis would offer an in-depth understanding of the financial implications related to the design, particularly in relation to redundancy and security.

Priority Balance:

The design prioritises security, scalability, and efficiency in relation to cost, redundancy, complexity, and efficiency balance. Strong security precautions, scalability through CIDR and subnetting, and the usage of

RIP for dynamic routing are prioritised over cost considerations. The benefits it provides to the resilience and performance of the network outweigh the complexity added.

Future Anticipation:

The design is positioned to address future organisational needs because it places a strong emphasis on security and scalability. As the business grows, the CIDR addressing system and subnetting offer a flexible framework for adding more offices and devices. By utilising RIP for dynamic routing, networks can become more flexible and easily expand to accommodate company expansion. Strong security protocols foresee the changing landscape of cybersecurity and guarantee that the network is safe from possible attacks.

An optimised network is vital to a business's sustainability and expansion because it creates the framework for increased operational effectiveness, flexibility, and scalability. The need for smooth connectivity and quick data transfer is become more and more important as technology develops. A network that is optimised not only keeps things running smoothly right now, but it also puts the company in a position to easily accept new developments and growth. Dynamic routing, effective IP address management, and thoughtful security measures enable the network to adapt to changing business requirements and become more flexible. One essential component of optimisation is scalability, which allows for the addition of new devices and features without sacrificing speed. An optimised network is a strategic asset in the dynamic digital world, enabling streamlined operations, stimulating innovation, and offering a strong foundation for long-term success.

Conclusion

This network design report outlines a methodical process for creating a scalable and robust infrastructure for the Manchester and London offices. A dedication to best practices is demonstrated by the use of CIDR IP addressing, dynamic routing using RIP, and strong security measures with SSH. Scalability is emphasised by the network's modular design, which supports wired and wireless connectivity. Nonetheless, it is advised to take into account improved redundancy, such as the addition of redundant lines or protocols, in order to further strengthen the network. A more thorough cost analysis would also offer a complete picture of the financial ramifications. Overall, the design effectively satisfies goals while placing a strong emphasis on efficiency, scalability, and security. It also provides a solid framework for the business's present and future networking requirements.

References

1. Farik, M. and Ali, A.S., 2015. Analysis of default passwords in routers against brute-force attack. International Journal of Technology Enhancements and Emerging Engineering Research, 4(9), pp.341-345.

2. Garimella, A.N.O.O.S.H.A. and Kumar, D.R., 2015. Secure Shell–Its Significance in Networking (SSH). International Journal of Application or Innovation in Engineering & Management, 4(3), pp.187-196.

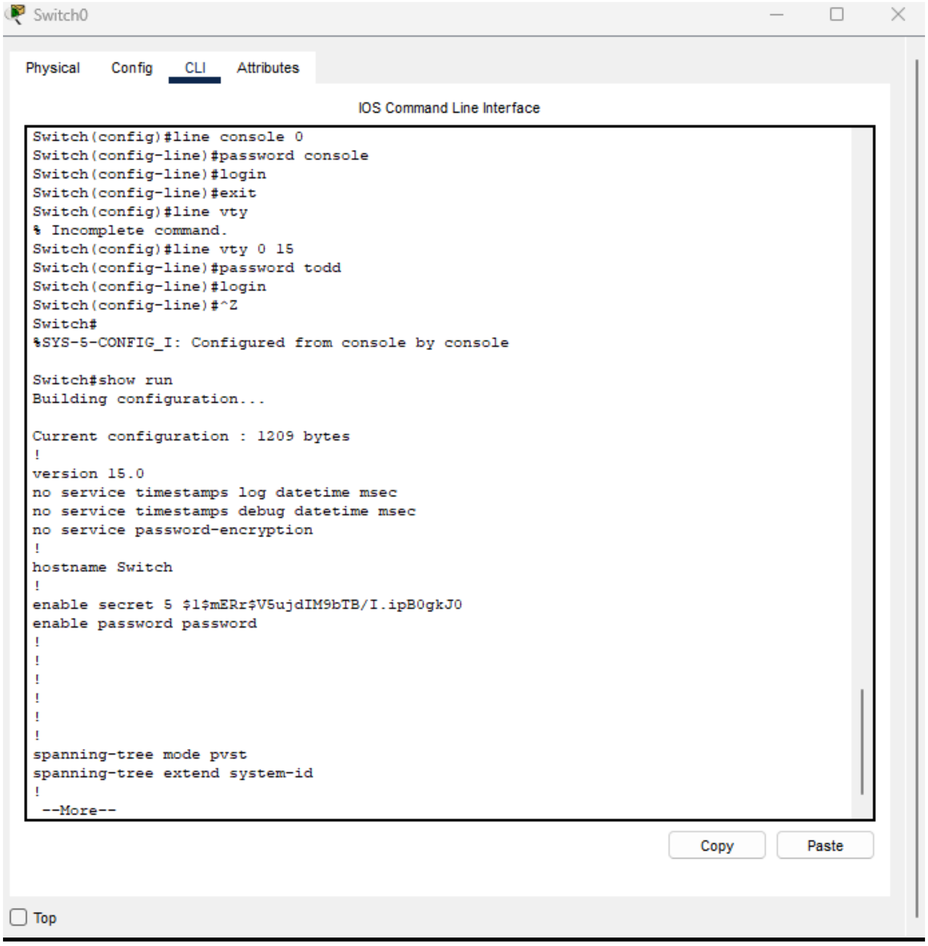
3. Yoo, K.J. and Kim, E.G., 2016. Design and implementation of DHCP supporting network attack prevention. Journal of the Korea Institute of Information and Communication Engineering, 20(4), pp.747-754.

4. Yang, S. and Yong, Z.Z., 2012, August. Rip internet protocol failure analysis and research. In *2012 International Conference on Industrial Control and Electronics Engineering* (pp. 1221-1224). IEEE.

5. Atefi, K., Shahin, A.H., Yahya, S. and Erfanian, A., 2016, August. Performance evaluation of RIP and EIGRP Routing Protocols in IEEE 802.3 u standard. In 2016 3rd International Conference on Computer and Information Sciences (ICCOINS) (pp. 209-214). IEEE.

6. Biradar, A.G., 2020, December. A comparative study on routing protocols: RIP, OSPF and EIGRP and their analysis using GNS-3. In 2020 5th IEEE international conference on recent advances and innovations in engineering (ICRAIE) (pp. 1-5). IEEE.

Appendix A



```
Switch(config)#line console 0
Switch(config-line)#password console
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty
% Incomplete command.
Switch(config)#line vty 0 15
Switch(config-line)#password todd
Switch(config-line)#login
Switch(config-line)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show run
Building configuration...

Current configuration : 1209 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$V5ujdIM9bTB/I.ipB0gkJ0
enable password password
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
 --More--
```

Switch configuration