Network Topology Design for

Company XYZ

SEAN-EDMUND ABABIO
[22483942]

Contents

Abstract

This report demonstrates an extensive network topology design for Company XYZ using Cisco Packet Tracer, which successfully fulfils all the requirements they established. The goal was to establish a medium-level secure network that links the offices in Manchester and London from different locations. A CIDR IP addressing scheme was successfully established to assign IP addresses and test connectivity across the network. All routers were configured with the proper protocols, including passwords for data encryption throughout the network to improve security. Each connection successfully met the operational needs and offered scalability for future expansion.

Introduction

As a network engineer I am in charge of building a network topology for Company XYZ and implementing the right configurations whenever necessary using Cisco Packet Tracer. Company XYZ has two bases in Manchester and London, the network I design must accommodate approximately fifty people and include twenty office desks in both cities with 10 hosts in each. In order to make sure everything functions properly and that the device hosts can communicate from different cities, I will also be confirming their connectivity and providing screenshots as proof. On one of the routers a secure shell password will be set up for extra security practices and remote access. A CIDR IP addressing scheme will be used to determine the IP address of the devices in use, RIP and DHCP configurations will be displayed and validated. To further demonstrate that everything is operating perfectly I will be showing every screenshot of the configuration and design aspects.

Aim and Objectives

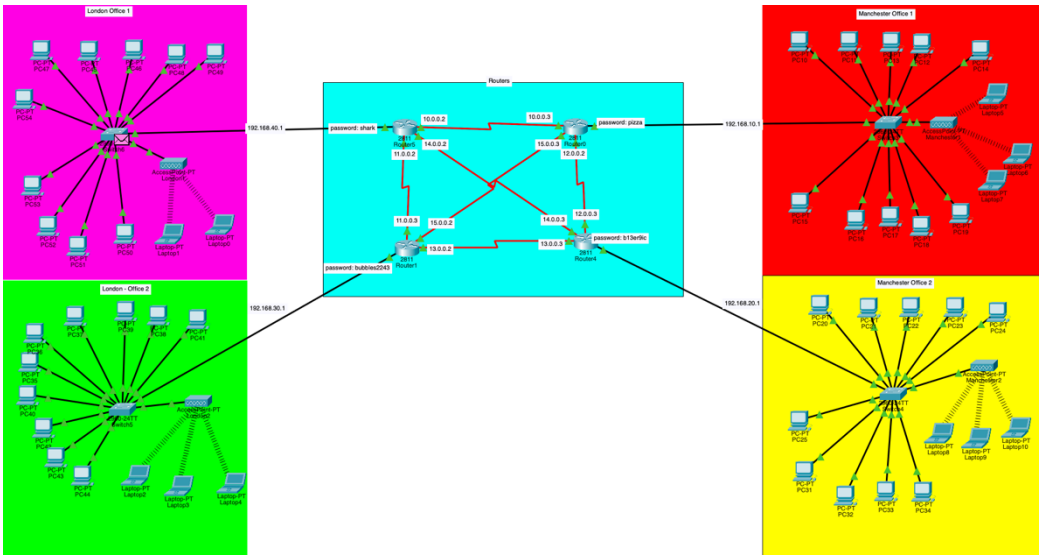
Aim:

Design a secure network topology for Company XYZ that connects both Manchester and London bases ensuring everything is fully functional and offers scalability.

Objectives:

- Design a medium-level network that connects the four offices
- Ensure wireless and wired connectivity is at all offices
- Verify and test the connectivity of the devices
- Use a CIDR addressing scheme to specify IP addresses
- Demonstrate and verify RIP and DHCP configurations
- Implement passwords on routers and SSH for remote access

Network Design



Wireless Access Points

As well as wired connectivity in all the offices I decided to implement wireless connectivity as well with the use of wireless access points for all the laptops, I decided to use access points rather than wireless routers since they can accommodate more connections, which is beneficial because office operations can continue uninterrupted.

Routers

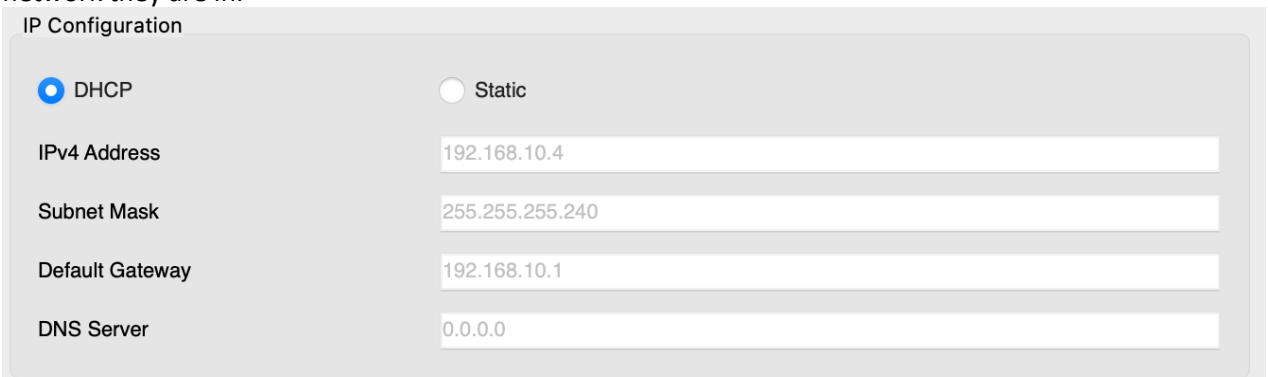
The network hub for all connections to the workplace is made up of four 2811 routers connected with serial DCE cables, which I installed. Since 2811 routers support routing protocols like DHCP and RIP, they were an excellent option for my implementation. Every router is password-protected to prevent unwanted access and to increase security. They are also very reliable, secure, and well-designed to facilitate communication between the different offices. I made some of the passwords complex with letters and numbers so that it makes it harder for malicious attackers to guess.

Switches

To enable several PCs to connect to each office's local network with copper straight through cables, I installed four 24-port switches in each office. These switches offer local connectivity and are easily expandable to accommodate additional devices if needed.

End Devices

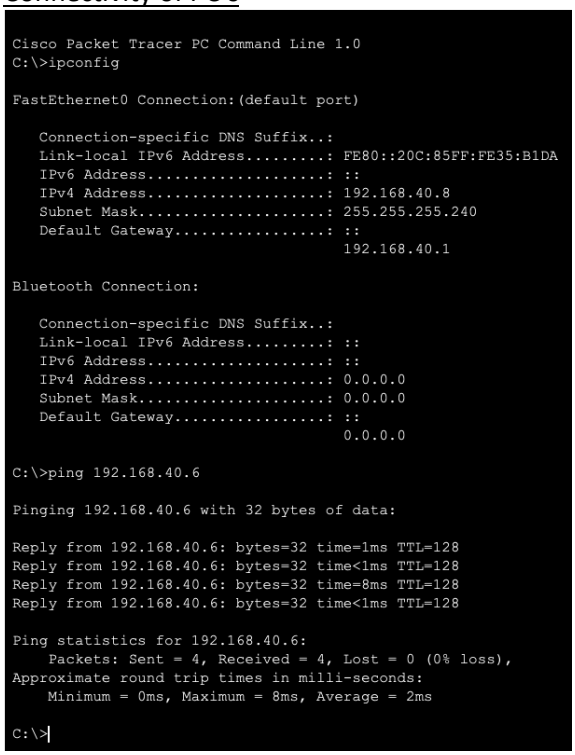
For the end devices that I used in each office I decided to use PCs and laptops, I believe that laptops were a good choice of devices to have alongside pcs because they are portable so employees wont have to be sat at one desk all the time and gives them flexibility on where to work anywhere around the room. All the PCs that are connected to the switch in each room have all got a unique Ip address depending on the network they are in.



In this screenshot this is one of the PCs from the Manchester Office 1, Every host has a unique IP address, which is assigned to the device after it is connected to the network using Classless Inter-Domain Routing. This allocation technique is commonly used to increase internet efficiency and flexibility (AWS, 2024).

192.168.10” represents the network that the PC is connected to, the last number at the end of that which is “4” is the host number and every device connected has a unique host number and it shows how many are connected to the network. Every router has a unique IP address that is used as the default gateway during configuration.

Connectivity of PC’s



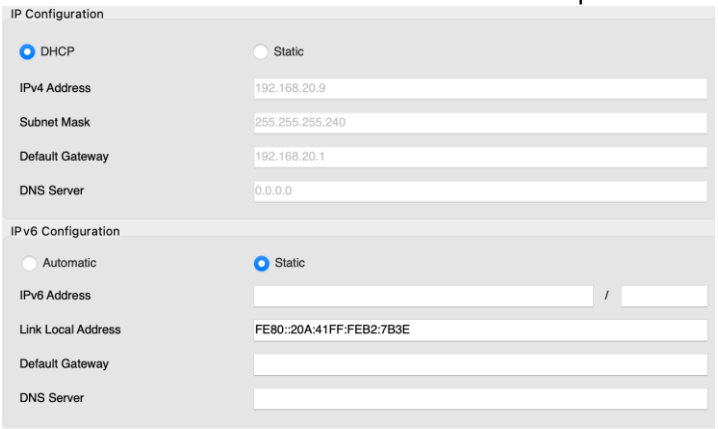
In this screenshot I have shown the connectivity of two Pcs from the same subnet, i used the ping command to ping the other PC and it shows that they received the message.

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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::204:9AFF:FEA3:CD87
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.40.10
   Subnet Mask.....: 255.255.255.240
   Default Gateway.....: ::
                                 192.168.40.1

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 192.168.10.8

Pinging 192.168.10.8 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.8: bytes=32 time=12ms TTL=126
Reply from 192.168.10.8: bytes=32 time=1ms TTL=126
Reply from 192.168.10.8: bytes=32 time=36ms TTL=126

Ping statistics for 192.168.10.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 36ms, Average = 16ms

C:\>
```

In this screenshot I have shown the connectivity of two Pcs from the two different subnets, I used the ping command to ping the other PC and it shows that they received the message.

DHCP

Dynamic Host Configuration Protocol is a protocol that automatically assigns a device an IP address related to the network as well as a subnet mask and default gateway. DHCP is good because it allows new devices to connect straight away without having to manually set an IP address and eliminates any IP configuration errors (Microsoft, 2021). In the screenshots below I have shown the configuration details for the DHCP on one of the routers and an example of it being used on a pc.



```
User Access Verification

Password:

Router>show running-config
          ^
% Invalid input detected at '^' marker.

Router>
Router>enable
Password:
Router#show running-config
Building configuration...

Current configuration : 1394 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime mse
no service password-encryption
!
hostname Router
!
!
!
enable password pizza
!
!
!
ip dhcp pool mypool
 network 192.168.10.0 255.255.255.240
 default-router 192.168.10.1
!
!

Router#
```

```
Password:

Router>
Router>show running-config
          ^
% Invalid input detected at '^' marker.

Router>
Router>enable
Password:
Router#show running-config
Building configuration...

Current configuration : 1394 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password pizza
!
!
!
ip dhcp pool mypool
 network 192.168.10.0 255.255.255.240
 default-router 192.168.10.1
!
!
!

Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            unassigned      YES unset  administratively down down
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
Serial0/2/0            15.0.0.3        YES manual up                    up
Serial0/2/1            unassigned      YES unset  administratively down down
Serial0/3/0            10.0.0.3        YES manual up                    up
Serial0/3/1            12.0.0.2        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

SSH

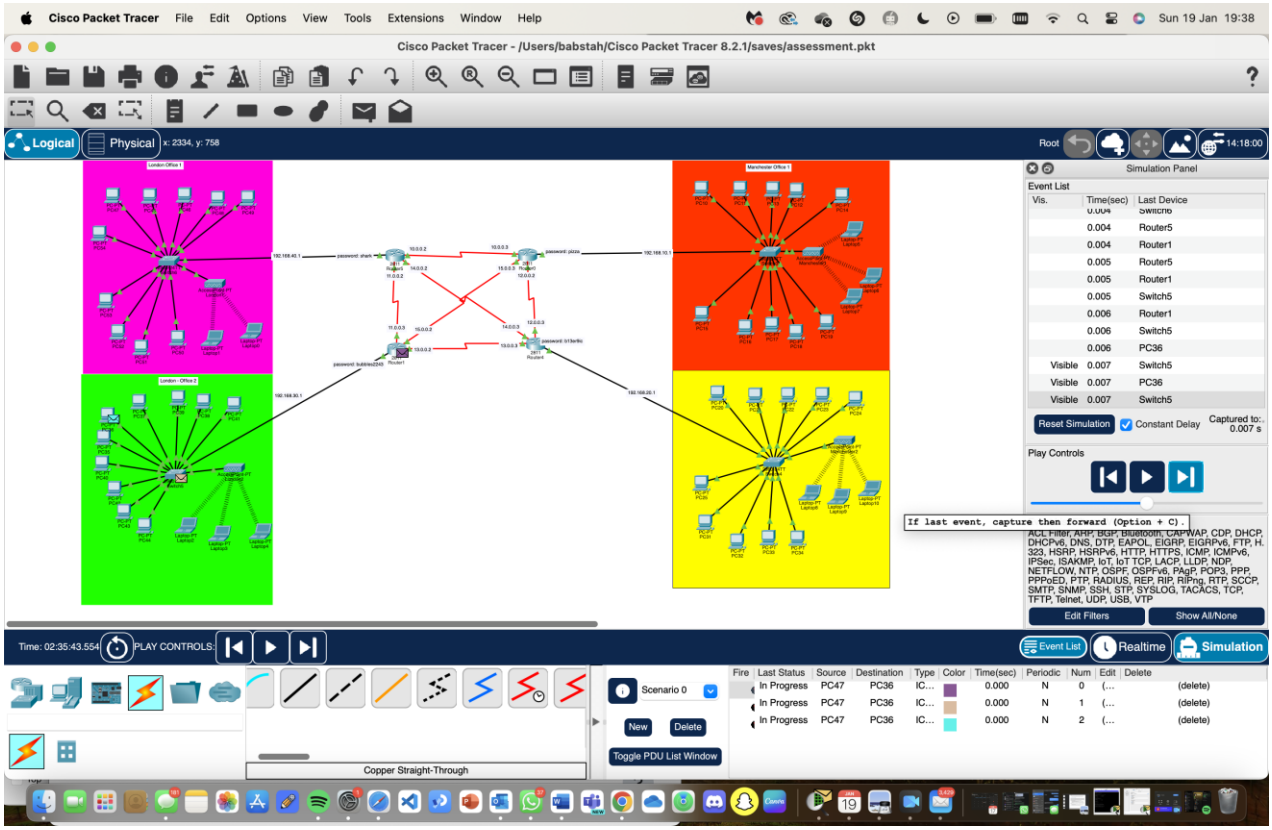
A network protocol called Secure Socket Shell offers a safe means to access content over unprotected networks, it typically uses a public key or password to verify access and encrypt connections between networks (Altaqi, 2020). I installed a secure shell on one of my routers and the screenshots below provide information on the state.

```
Password:

r1>show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
r1>show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
r1>show running-config
        ^
% Invalid input detected at '^' marker.

r1>show running config
        ^
% Invalid input detected at '^' marker.

r1>enable
Password:
Password:
r1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
r1#show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
r1#show running-config
Building configuration...

Current configuration : 1533 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname r1
!
!
!
enable password bl3er9ic
!
!
!
ip dhcp pool mypool2
 network 192.168.20.0 255.255.255.240
 default-router 192.168.20.1
!
!
!
no ip cef
no ipv6 cef
```

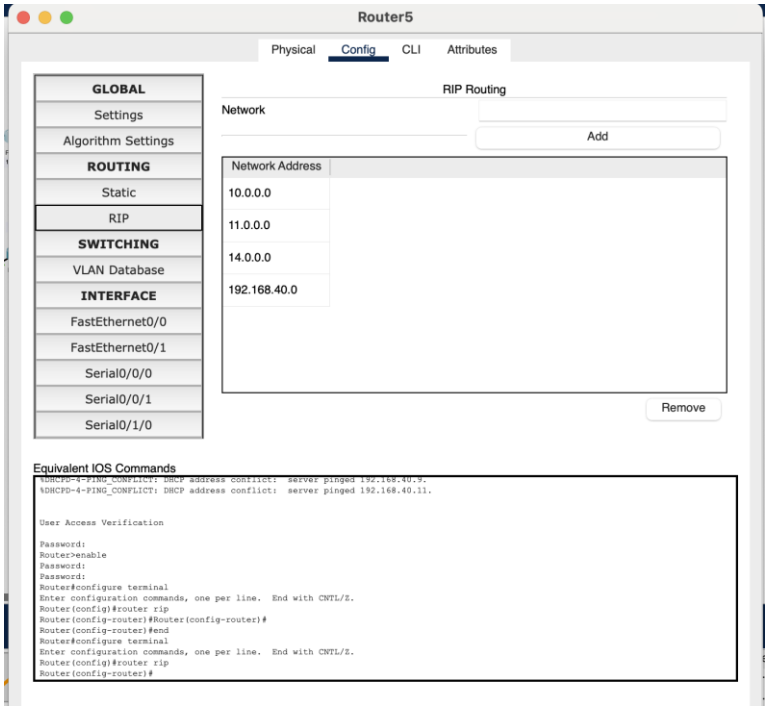
```
Password:
Password:
r1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
r1#show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
r1#show running-config
Building configuration...

Current configuration : 1533 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname r1
!
!
!
enable password bl3er9ic
!
!
!
ip dhcp pool mypool2
 network 192.168.20.0 255.255.255.240
 default-router 192.168.20.1
!
!
!
no ip cef
no ipv6 cef
!

r1#ssh -l r1 192.168.20.1

Password:
% Login invalid


Password:
% Login invalid


Password:

[Connection to 192.168.20.1 closed by foreign host]
r1#
```

RIP

Routing information protocol is a routing protocol that is most efficient path for transmitting packets across a network by using a hop count (UniNets, 2024), this protocol is typically used rather than a different one for transmitting because it is simple to configure and manage and it is also widely supported on multiple platforms (Wikipedia, 2021). I have shown below an example of it in my network topology:



As you can see it show it is successfully working in the bottom right.



Network Evaluation and Discussion

I believe that my network topology has successfully met all the requirements of the company and is configured very well, both Manchester and London bases have got two offices each which I have used a

range of cables like copper straight through and serial DCE to connect them with PC's, switches and routers. The routers form the network's core, providing interconnection across offices. The routers also have passwords (b13er9ic, bubbles2243), indicating that security procedures are in place, and at least one of them has a secure shell for remote access. Each office has its own subnet with wired and wireless connections on all desks, which was one of the task's objectives; for example, 192.168.10.0 is a subnet that represents the Manchester office 1 network. Since each office only has one switch, one of my topology's weaknesses is the possibility of single points of failure. This could be problematic because if the switch ever shuts down, all of the devices in that network would lose connectivity which could lead to data loss. One solution would be to have two office sections with the same number of hosts but two different switches. Redundancy among the connected routers is one of my topology's advantages this helps the business by enabling traffic to flow through alternate routes in the event that any routers or links within it fail. Another improvement is that I may also use devices like tablets and smartphones when connecting wirelessly to make it more cost effective rather than using laptops which can vary on price.

Conclusion

All things considered, this assignment from the company truly improved my skills as a network engineer. I was able to show off a multi-connection network on my own and demonstrated innovative methods like configuring DHCP and RIP and password protecting the routers for added security. Along with recognising what I did successfully for my network, I now know where it needs to be improved to make it more secure. The network will become more dependable and enterprise-friendly when I put the previously described improvements into practice, which will enable the business to grow further in the future, if they so want.

References

Altaqi, W. (2020). *The What, Why & How of SSH Protocol*. [online] Keyfactor. Available at: https://www.keyfactor.com/blog/ssh-protocol/ [Accessed 19 Jan. 2025].

AWS (2024). *What is CIDR? - CIDR blocks and notation explained - AWS*. [online] Amazon Web Services, Inc. Available at: https://aws.amazon.com/what-is/cidr/ [Accessed 19 Jan. 2025].

Microsoft (2021). *Dynamic Host Configuration Protocol (DHCP)*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top [Accessed 19 Jan. 2025].

UniNets (2024). *Routing Information Protocol (RIP) in Computer Networks*. [online] https://www.uninets.com/UniNets. Available at: https://www.uninets.com/blog/routing-information-protocol [Accessed 19 Jan. 2025].

Wikipedia. (2021). *Routing Information Protocol*. [online] Available at: https://en.wikipedia.org/wiki/Routing_Information_Protocol.