GROUP ASSIGNMENT

COMP40002

NETWORKING CONCEPTS AND CYBER SECURITY- 1

CF23A1COM/CFK23A1COM

HAND OUT DATE: 2nd week

HAND IN DATE: ASSIGNMENT2: 09-02-2024

WEIGHTAGE: ASSIGNMENT 1: 50%

INSTRUCTION TO CANDIDATES:

1. **Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).**
2. **Late submission will be awarded zero (0) unless Exceptional Circumstances (EC) are upheld.**
3. **We draw your attention to the Academic Conduct Procedure to encourage good academic practice.**
4. **Assignment presentation and modeling work should be submitted as a softcopy**

Acknowledgement

We would like to express our heartfelt appreciation to Mrs. Krishnadewa, our lecturer, for his invaluable support and guidance throughout this assignment. His assistance and encouragement were crucial in ensuring the timely completion of this report.

We also extend our thanks to our peers for their help and support, which contributed significantly to the successful outcome of this project.

Group Members

Name	CB Number	Role
Nipul Mallikarachchi ----------	CB011999	Configuring routers(HSRP) / (NAT/PAT)
Nethin Panapitiya ----------	CB014062	Creating VLANs/Assigning ports accordingly
Shankarshana Ratnasabapathy --	CB011326	Subnetting/Designing the Topology/Securing
Aaqib Ashan ----------	CB013069	Configuring Switches/ IP DHCP

Table of Content

Table of Figures

1. Network Infrastructure Overview and Design Strategy

This report will outline the process of creating two distinct networks while developing the network infrastructure tailored to the specific needs of the company, which is currently experiencing sluggish performance and has locations in Manchester and Birmingham. The design consists of three separate networks connected by routers. One router facilitates communication with external servers, while the other two address the specific needs of each city branch, improving data transfer and communication efficiency.

In this network, two geographical locations—more precisely, two branches—are connected by WAN technology. Because of the slowness of the current infrastructure, a substantial improvement from the previous 100 Mbps throughput is now available—one Gbps.

There are several WAN technologies available, MPLS (Multiprotocol Label Switching) being one of them. Compared to other options, MPLS provides a private, dependable connection with consistent performance, but at a possibly higher cost and longer deployment time.

Internet VPN is an additional choice that is well-known for being widely accessible and reasonably priced. Its performance might not always be reliable, though.

Conversely, SD-WAN offers improved application performance and flexibility, but it is dependent on internet connections, which may result in performance fluctuations.

Finally, symmetrical bandwidth is provided via leased lines, making them appropriate for large bandwidth needs. However, they can be expensive, and if something changes, you could need more physical circuits.

The Manchester side's primary IP address is 192.16.0.0/24, or 11000000.00010000.00000000.00000000 in binary format. We need four subnets, with subnet masks of 255.255.255.192, namely 192.16.0.0/26, 192.16.0.64/26, 192.16.0.128/26, and 192.16.0.192/26, to support the network's separation into four segments.

The primary IP address for the external domain is 172.16.0.0/24. With a corresponding subnet mask of 255.255.255.224, this subnet is further divided into five subnets: 172.16.0.0.0/27, 172.16.0.32/27, 172.16.0.64/27, 172.16.0.128/27, and 172.16.0.192/27.

The primary IP address for the Birmingham side is 192.17.0.0/24. Similar to that, it uses a subnet mask of 255.255.255.192 to divide itself into four subnets: 192.17.0.0/26, 192.17.0.64/26, 192.17.0.128/26, and 192.17.0.192/26.

2. Wireless Access Point Security and VLAN Configuration

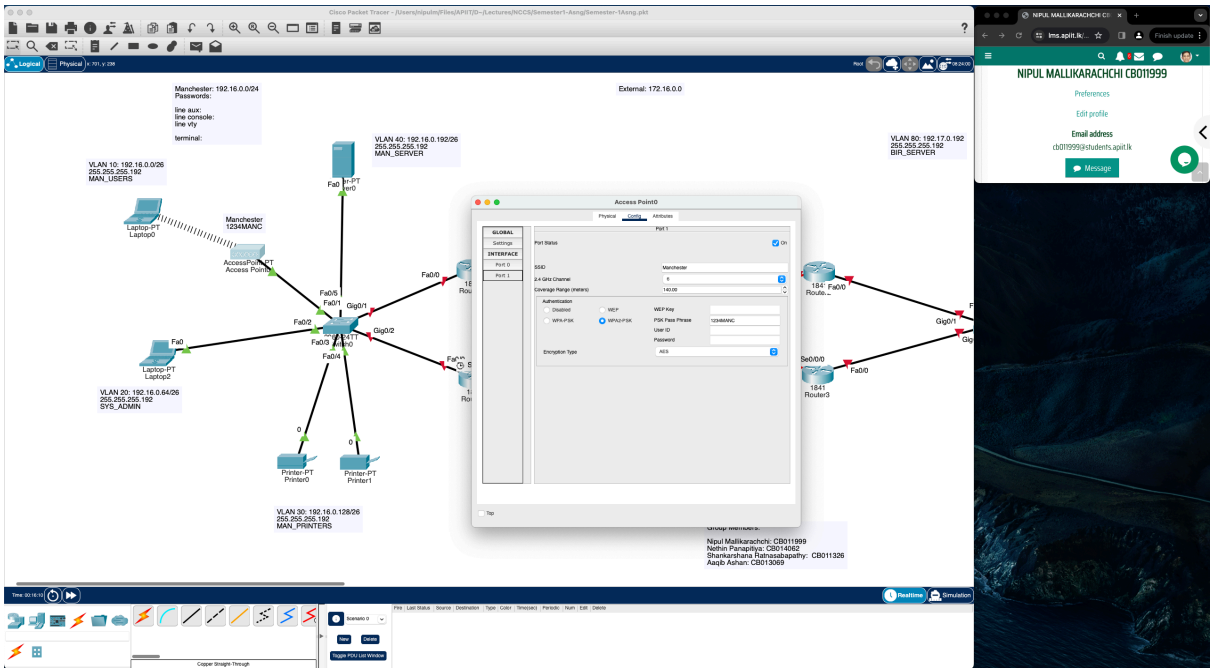


Figure 1

In the provided screenshot, we are assigning a distinct name and password to the wireless access point, enhancing the security of the network. This measure ensures that only authorized devices, such as those used by company employees, can connect using the designated name and password. For the Manchester branch, we have designated the name "Manchester" with the corresponding password "1234MANC." Access to the network is restricted without these credentials, preventing unauthorized users from connecting. Similar security measures are applied to the access point in Birmingham, following the same process to safeguard the network in both locations.

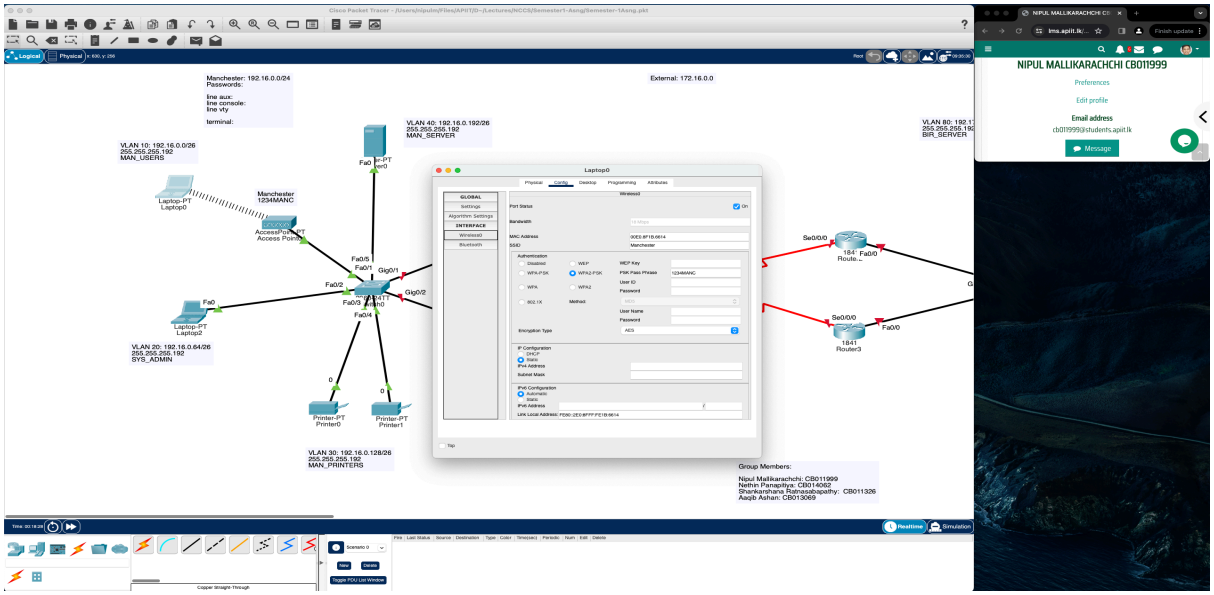


Figure 2

As previously stated, the process of connecting a device to an access point includes configuring the device settings. To connect to the access point, users must first navigate to their device's configuration settings and enter the specified name and password. This authentication method ensures secure and controlled network access by requiring users to provide the proper credentials for successful connectivity.

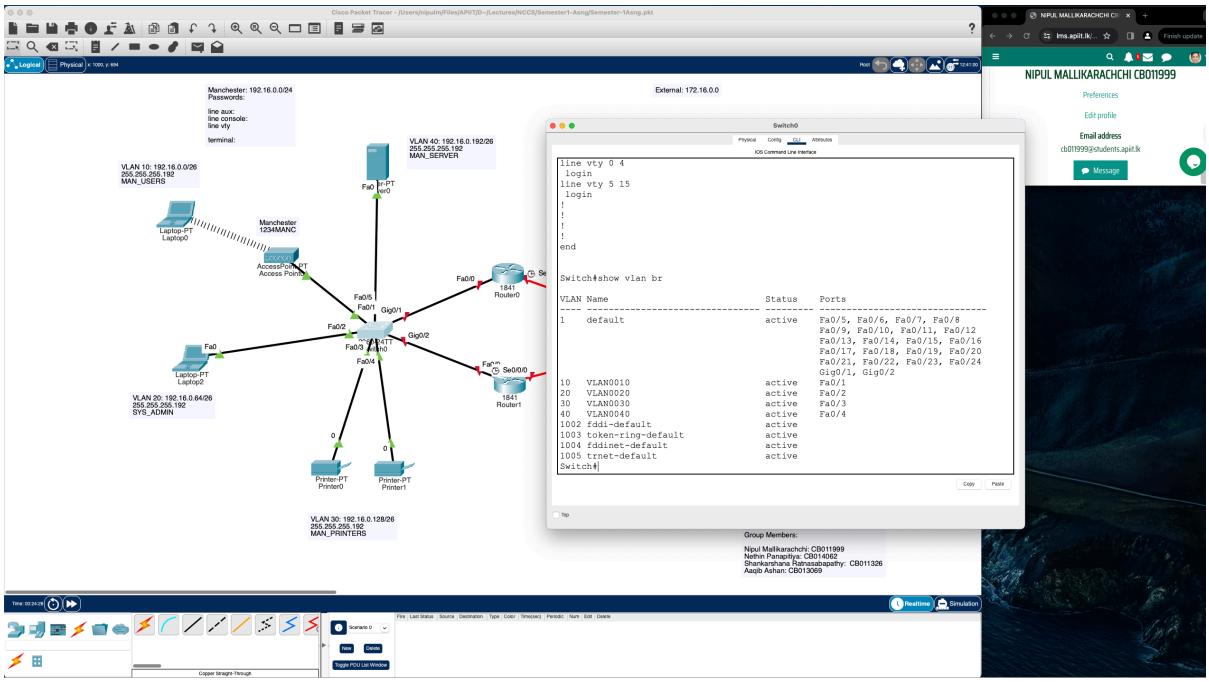


Figure 3

To improve network management, each branch (Manchester and Birmingham) now has four VLANs configured. These VLANs are set up for administration, local servers, printers, and general user access. Corresponding Fast Ethernet cables have been assigned to each VLAN, ensuring that devices connected to specific cables are automatically classified within the appropriate VLAN, streamlining network organisation and administration.

Assigning VLANs to specific Fast Ethernet cables involves using the "switchport" command, specifying the VLAN name, and utilizing the "switchport access" command within the Fast Ethernet interface configuration. This ensures devices connected to these cables are associated with the designated VLAN.

In the case of router-to-switch connections, the "trunk" command is employed to facilitate the transfer of traffic between VLANs, ensuring seamless communication across the network.

Fast Ethernet ports 0/6 to 0/20 are intended to connect end devices for users coming from the switch, using copper straight-through cables for VLAN 10. In accordance with the report's strategy of combining wired and wireless connections for the same user category within a single VLAN, both wired end devices and wireless access points share VLAN 10. The configuration approach is similar to the previous process, with the "range" command used to efficiently include all connections at once. This ensures streamlined network administration for the specified user category by combining wired and wireless connections into a single VLAN structure.

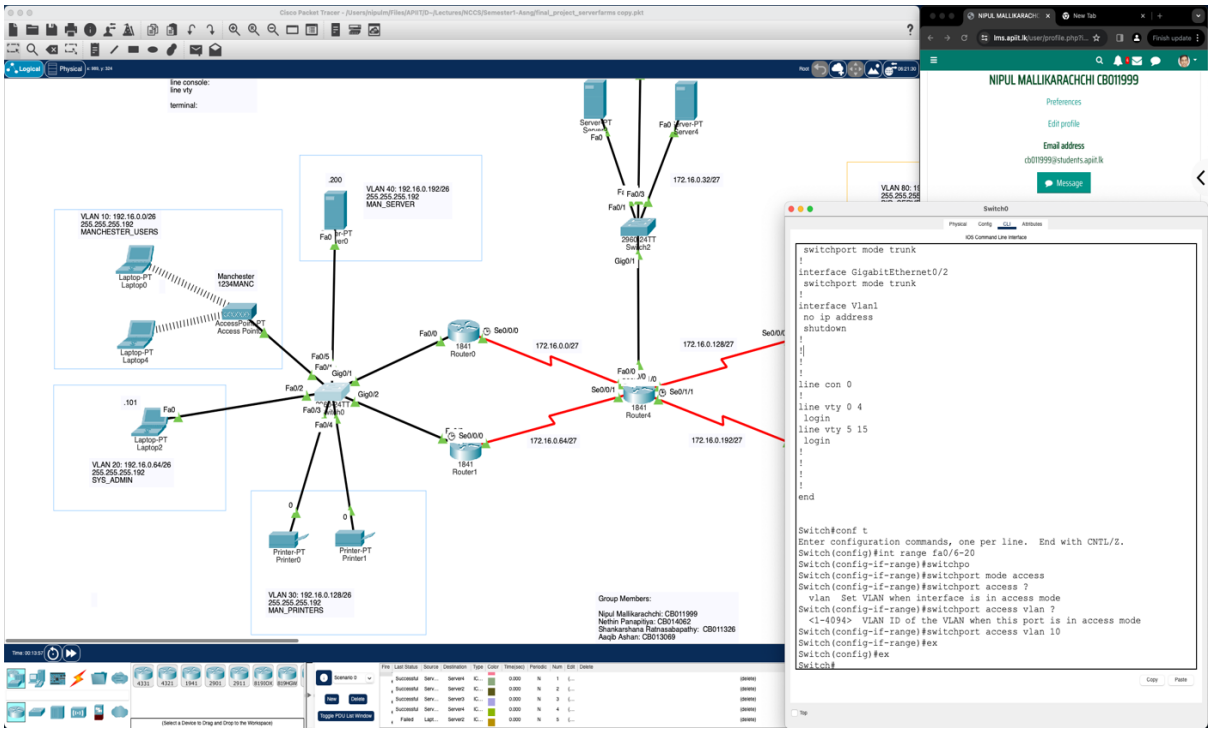


Figure 4

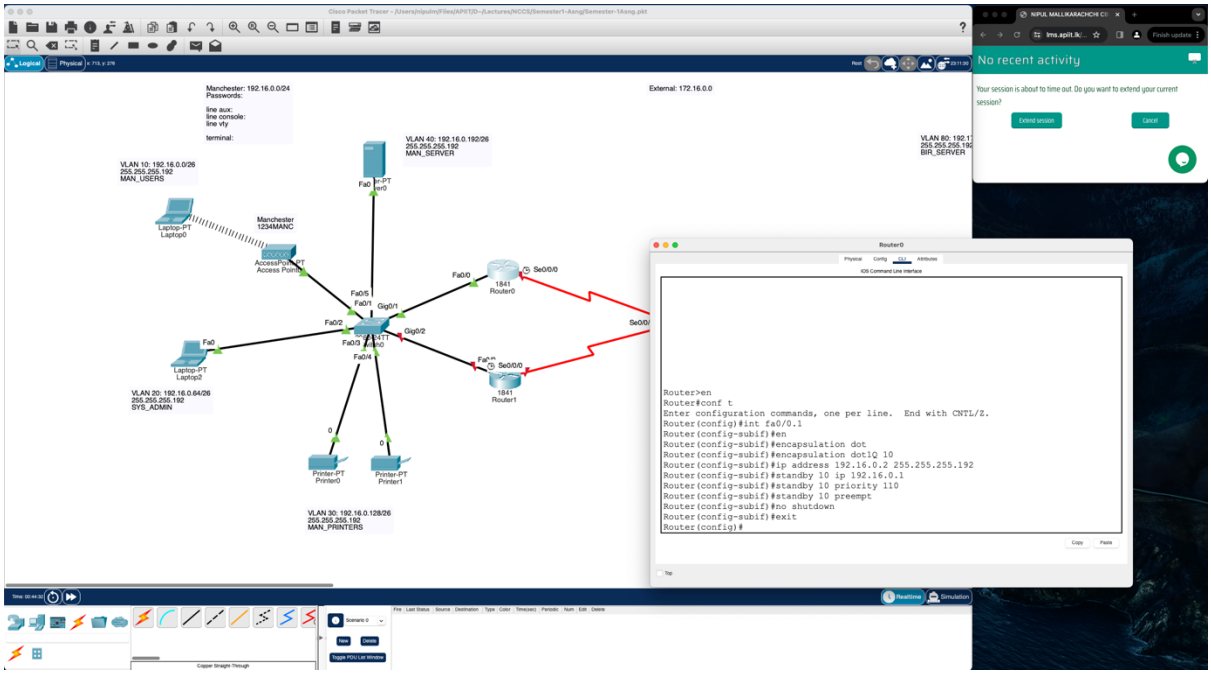


Figure 5

To establish WAN topology and ensure network redundancy, we initiate the setup by activating the Fast Ethernet cable connected from Router 0 to the switch using the "no shutdown" command. The Fast Ethernet 0/0 interface is then divided into four sections (cables) for each VLAN. Within each VLAN interface, we use the "encapsulation DOTQ10 10" command, creating a group (designated by the "10").

For each VLAN interface, specific IP addresses are assigned along with a standby IP serving as the default gateway, distinct from any device IP. As the primary router, Router 0 is configured with a priority of 200, "preempt," and "no shutdown" to activate the created segment of the Fast Ethernet port. This process is repeated for all four VLANs, with different group names assigned to the other three VLANs. The comprehensive configuration ensures that the router becomes the main router, enhancing network reliability through redundancy in the event of a router failure.

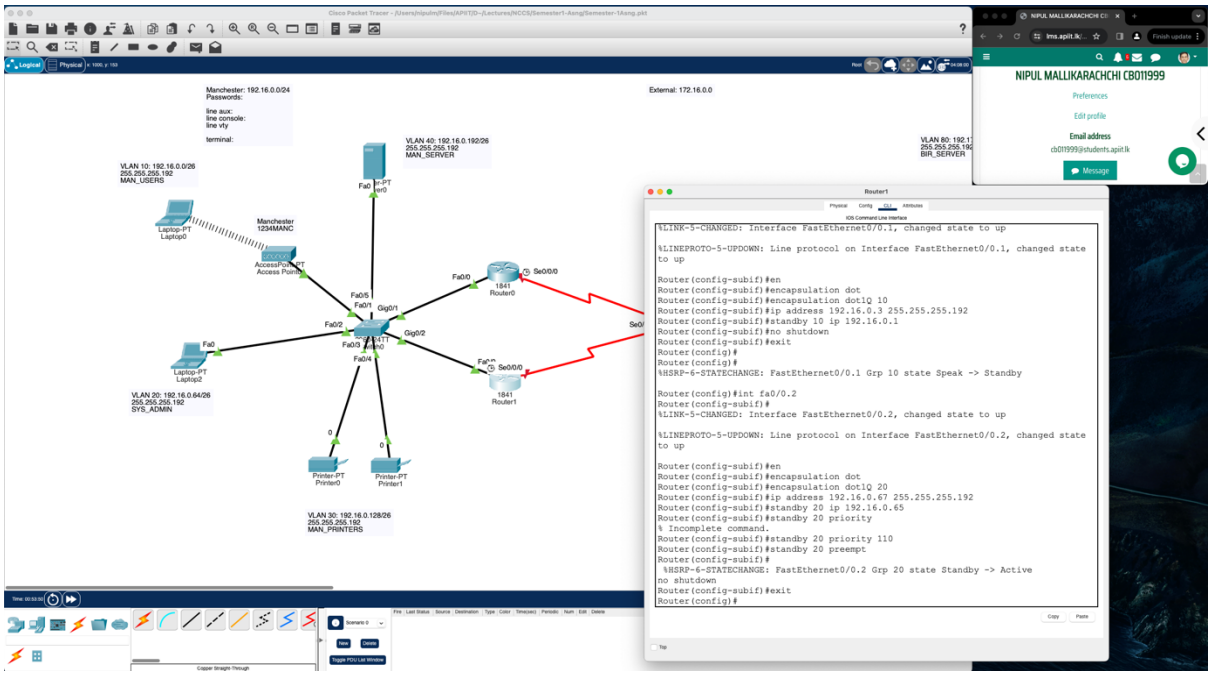


Figure 6

In configuring the standby router, the process closely mirrors that of the main router, with the main Fast Ethernet cable activated and divided into four sub-cables. However, in the standby router, unique IP addresses are assigned for each VLAN, while the standby IP address remains consistent within a specific VLAN. Unlike the main router, the standby router doesn't use the "priority" and "preempt" commands, as it operates in a standby capacity.

3. WAN Topology and Redundancy Implementation

We implemented IP DHCP to automate the assignment of IP addresses to connected devices, thereby eliminating the need for manual IP assignments. When creating an IP DHCP pool, such as "MANCHESTER_USERS," you must specify a network IP address and a default gateway, as well as exclusions to prevent certain IP addresses from being used. DHCP is used for user VLANs, while static IPs are used for the remaining three VLANs, which have fewer devices that change or expand. Static IP addresses limit network access to specific devices within the designated VLAN, which improves security.

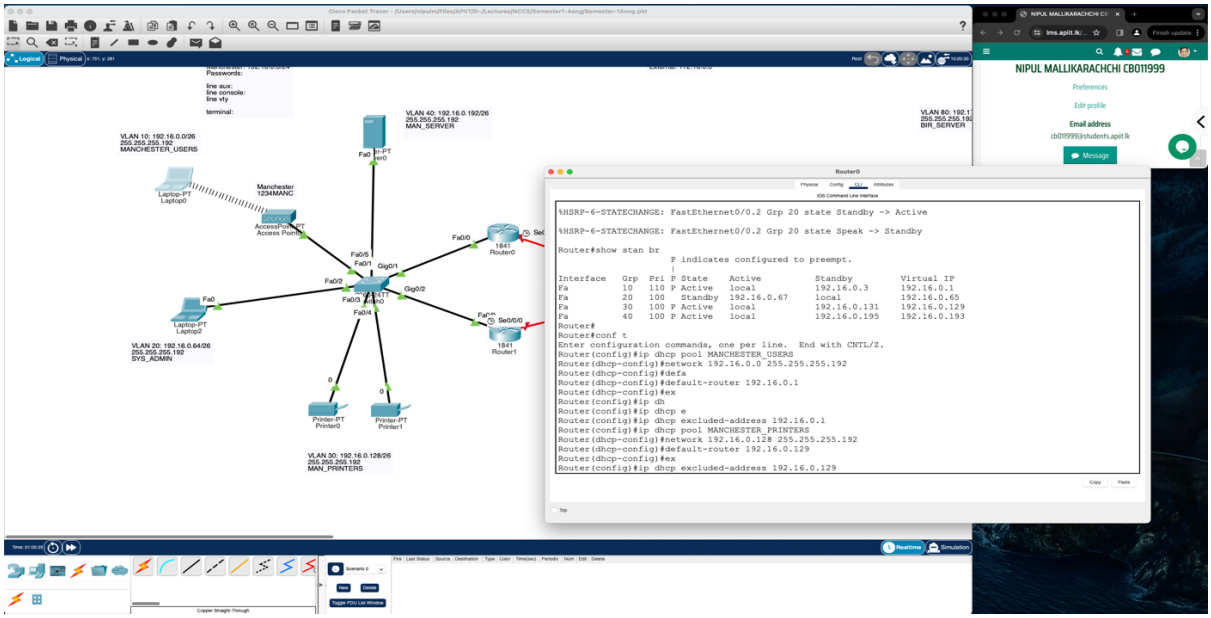
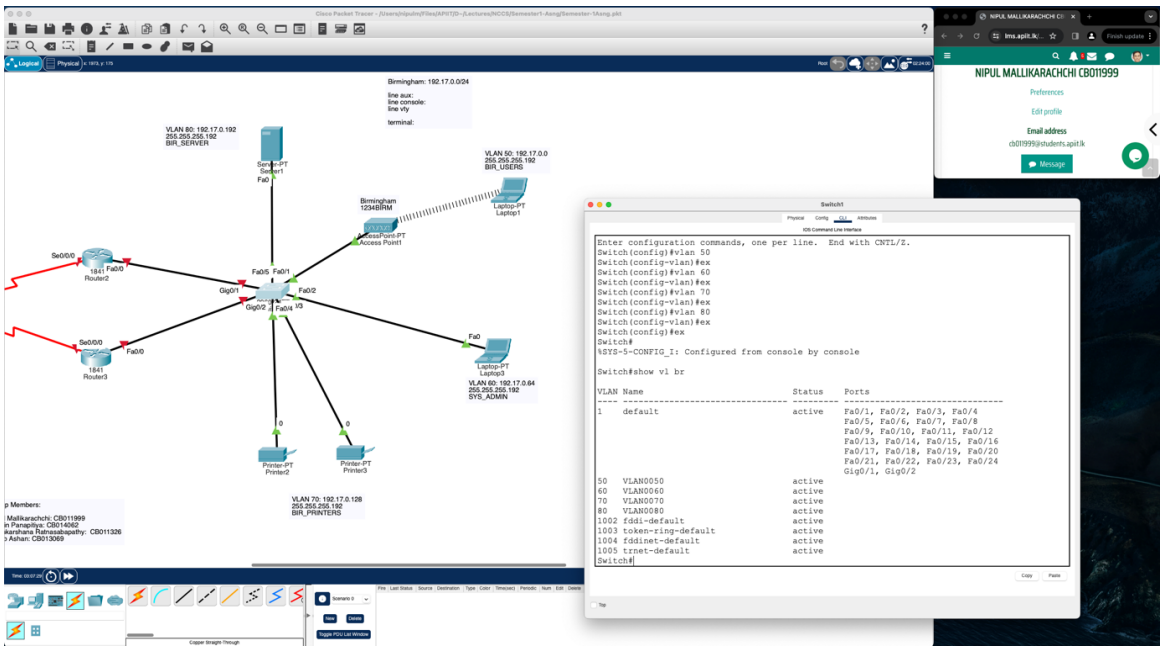


Figure 7

Regarding the Birmingham network, the implementation includes security measures for the wireless access point to prevent unauthorized access and protect sensitive data from potential breaches. To achieve this, a strong password is crucial, ensuring access is granted only to authorized individuals.



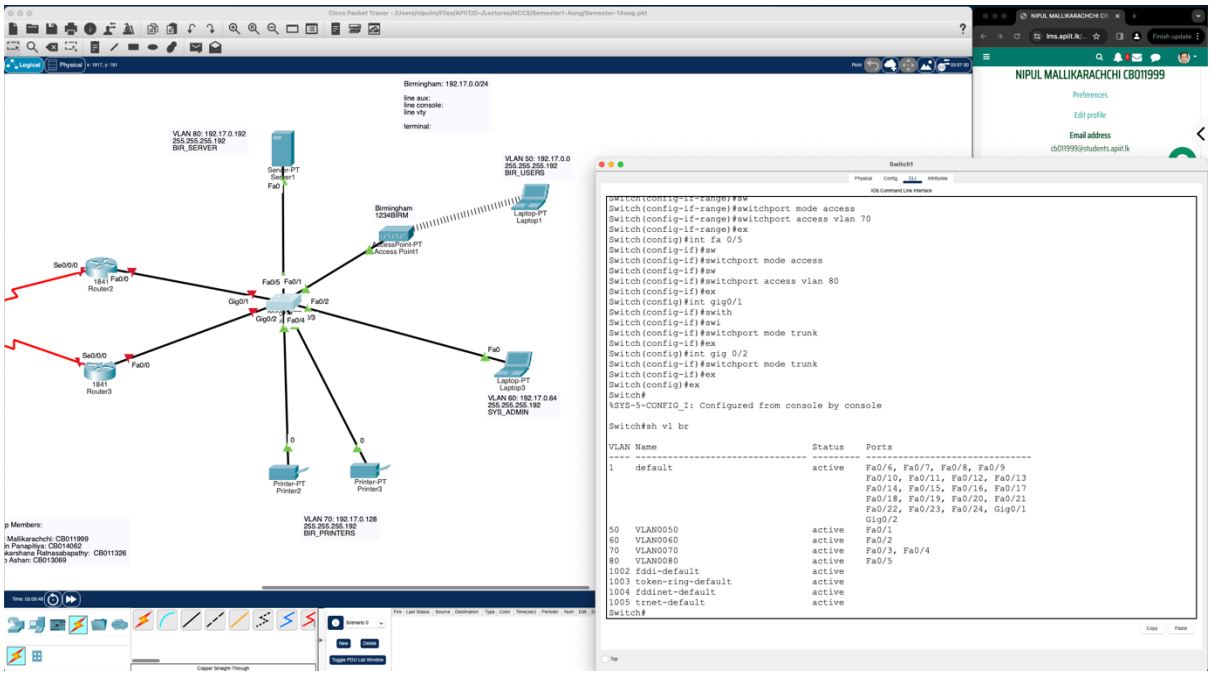


Figure 9

The network structure for Birmingham closely resembles that of Manchester, and the procedures largely align. Initial steps involve assigning Fast Ethernet ports to dedicated VLANs, establishing a foundation for organized network management.

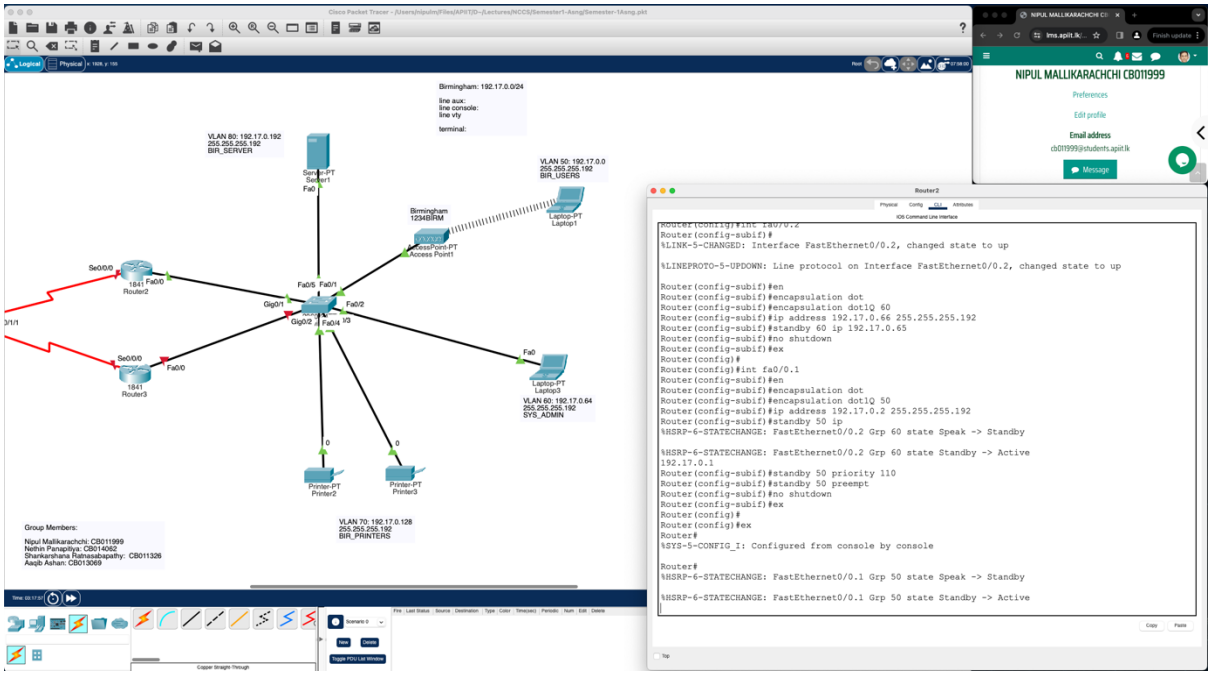


Figure 10

Initiating the setup, the Fast Ethernet cable connecting Router 0 to the switch is activated using the "no shutdown" command. This connection is established through Fast Ethernet 0/0. The port is then segmented into four distinct sections (cables), each designated for a specific VLAN.

Within the Fast Ethernet interface configuration, the "encapsulation DOTQ10 50" command is applied, indicating the creation of a group identified by the number 50. Assigned IP addresses for each VLAN and standby IPs as default gateways are configured. Given its role as the main router, a priority of 200, "preempt" command, and "no shutdown" prompt are assigned to activate the configured segment of the main Fast Ethernet port.

This comprehensive process is replicated for all four VLANs, ensuring appropriate IP assignments and standby configurations. Notably, the group names differ for the other three VLANs, resulting in the successful configuration of the main router for the network.

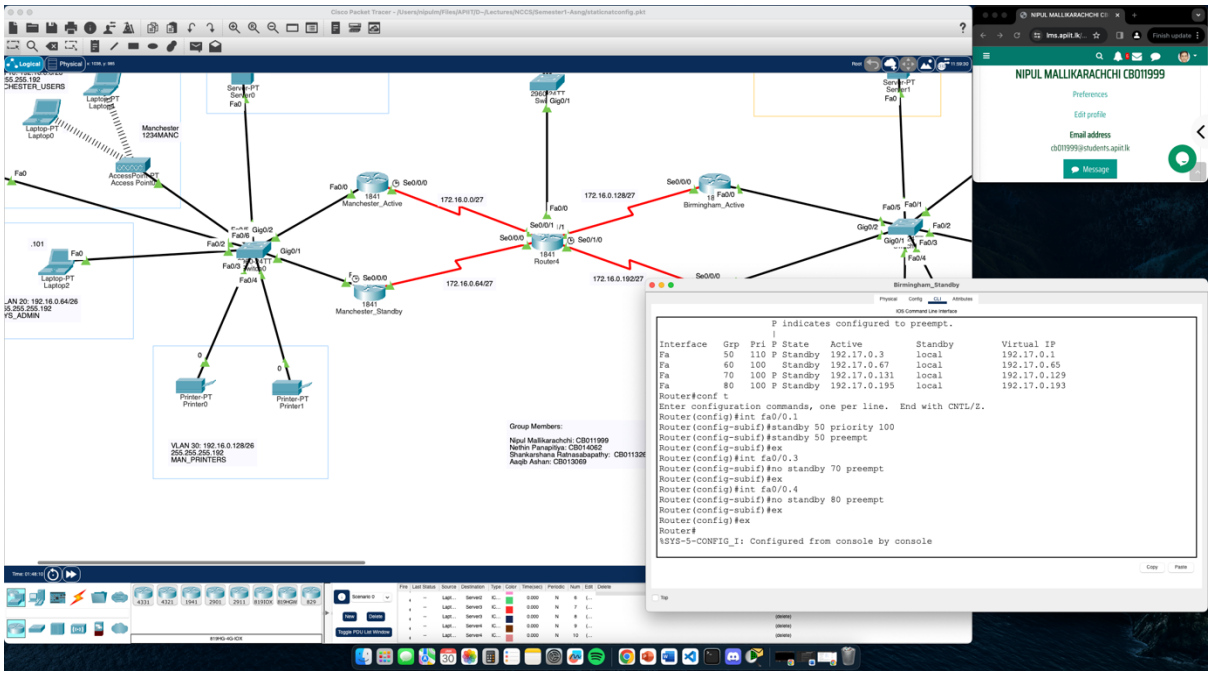


Figure 11

In the event of a main router failure or technical issues, the standby router takes over as the backup and becomes active. The standby router's configuration is nearly identical to the main router's, with the main Fast Ethernet cable activated and divided into four sub-cables. Notably, the standby router cannot use the same IP addresses for each VLAN; however, the standby IP address is consistent within a single VLAN. The priority is set to lower than that of the active router.

Following that, the IP DHCP configuration for Birmingham is implemented. To prevent usage, an IP DHCP pool named "BIRMINGHAM _USERS" is created, which includes the network IP address and an excluded default gateway. IP DHCP is applied selectively to user VLANs, while static IP addresses are assigned to the remaining three VLANs, where devices are unlikely to change or expand. This strategy increases security by limiting network access in those VLANs to specific devices.

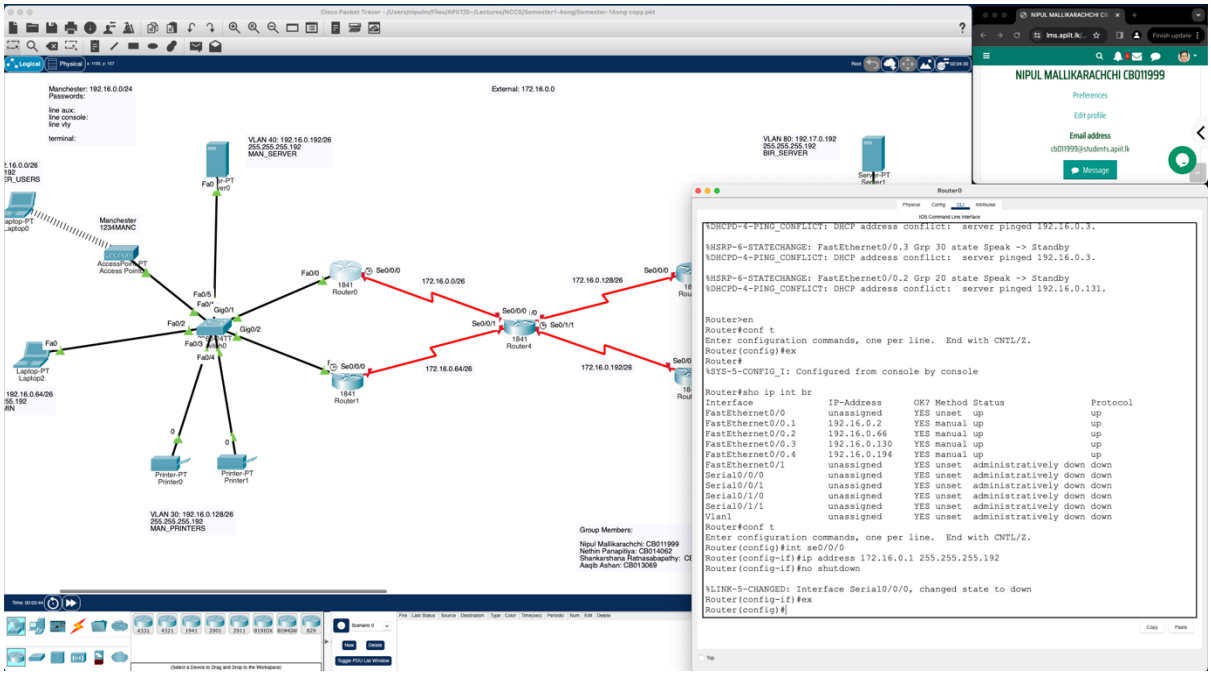


Figure 12

To enable connectivity, we configure the serial interface port by assigning an IP address (172.16.0.1) to the connection between the main router and Router 0. The "no shutdown" command is used to activate the port. This process is repeated for the standby router, ensuring that both routers are operational. Similarly, for Birmingham, the serial interface port is configured with an assigned IP address, activated using "no shutdown," and then verified to ensure its active status.

Additionally, the "Nat inside" command is implemented to enable network translation, particularly for the static IP section of the network. This configuration is essential for translating responses when pinging from one network to another. Due to the dynamic nature of IPs in the DHCP pool, responses will reflect one of the multiple IPs in the pool, offering a consistent and reliable network translation mechanism.

4. Network Connectivity and IP Routing

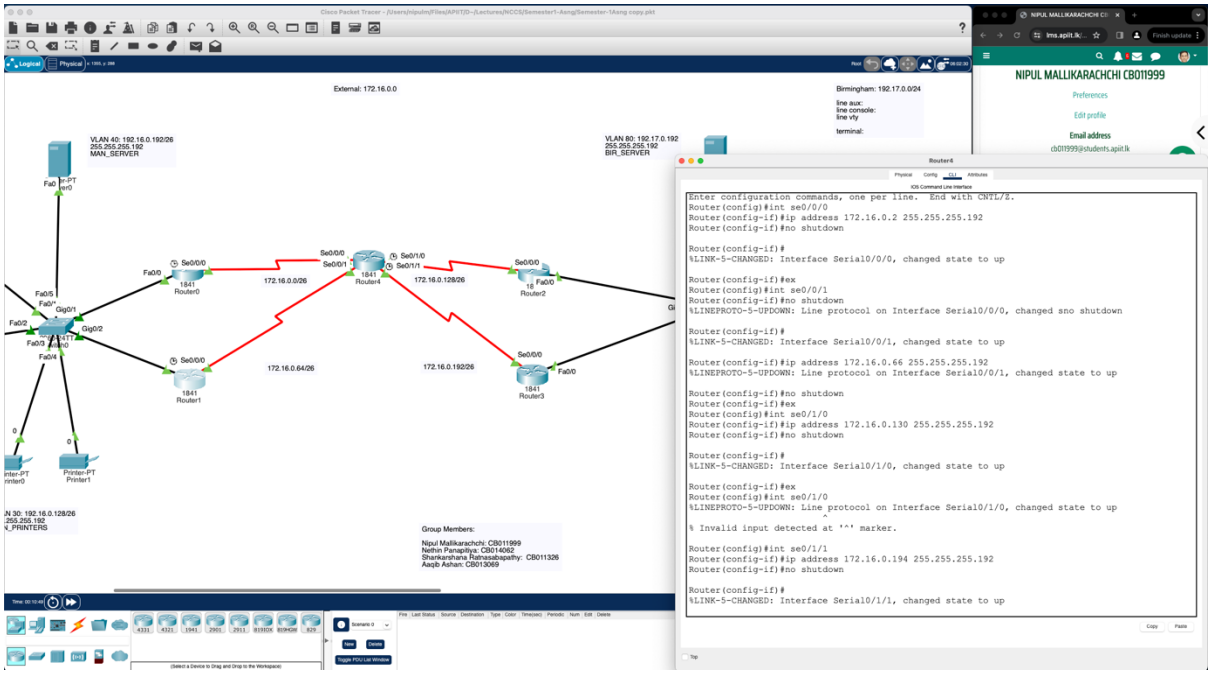


Figure 13

The main router, which connects the other four networks, is a critical component of the network infrastructure. To configure this connectivity, navigate through each serial port, assigning designated IPs individually, and then using the activation command "no shutdown" to ensure operational status across all ports.

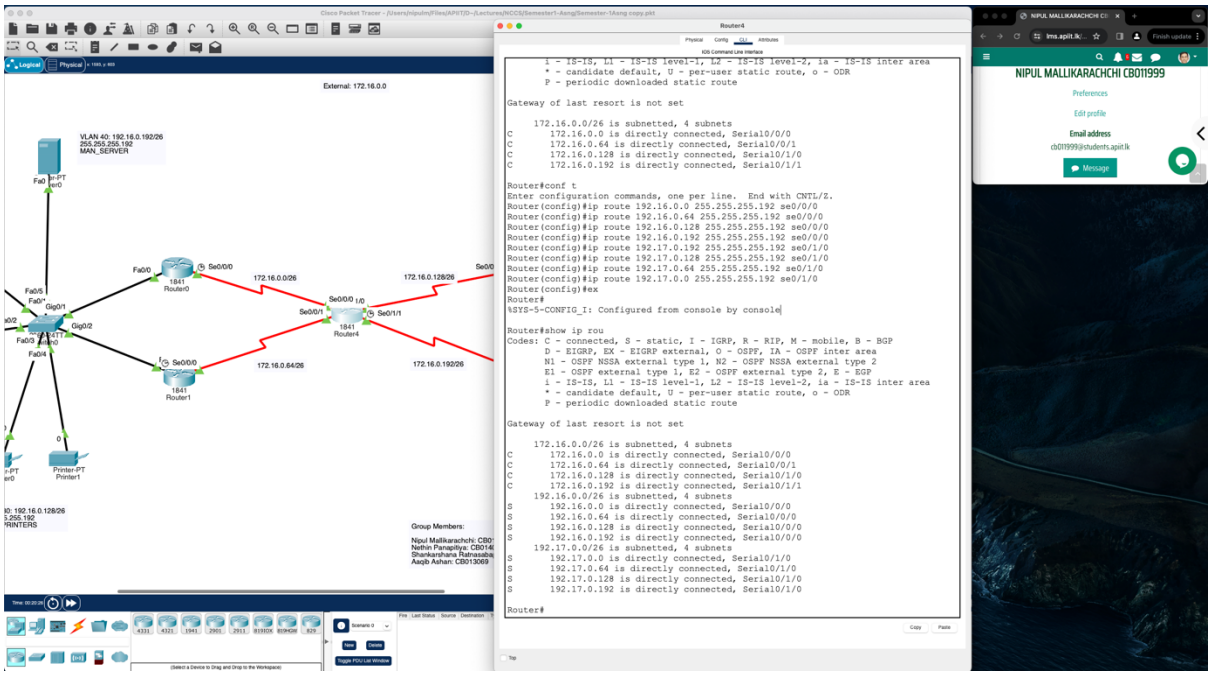


Figure 14

Moving forward, IP routing is necessary to relay information about unknown networks to routers. The main router needs to be informed about networks in both cities, totaling eight different network IP addresses. The same approach is applied to the remaining four routers for a comprehensive understanding of the network landscape.

5. Data Security and External Server Farm Setup

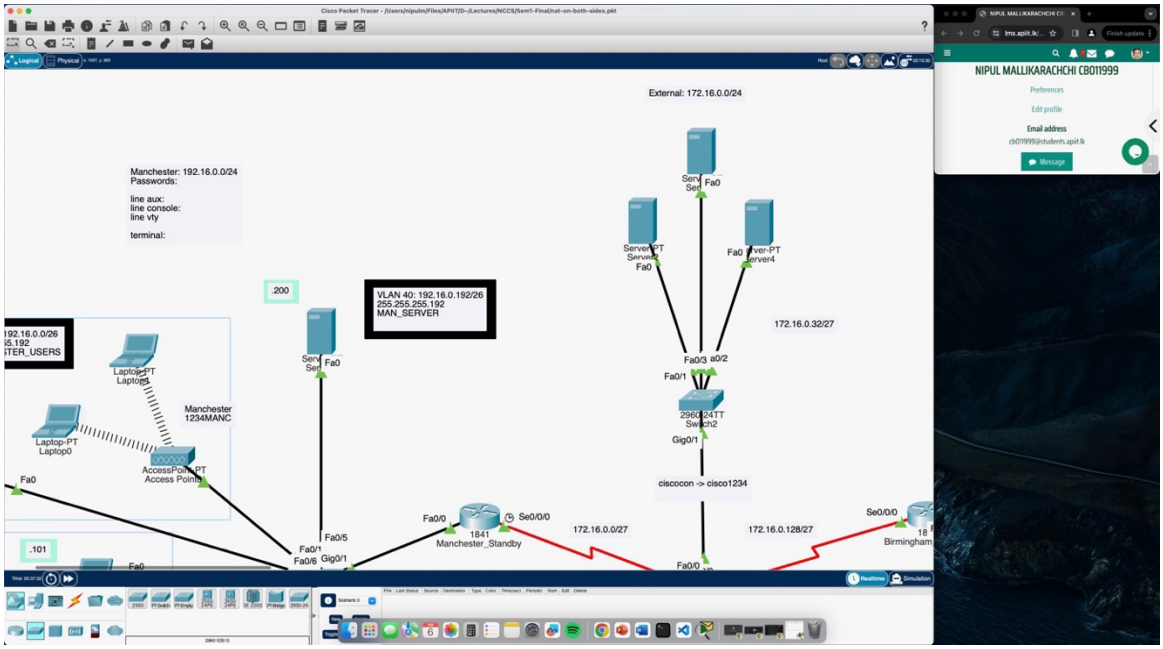


Figure 15

In order to strengthen data security, an external server farm is established, which serves as a dual repository for data storage both internally and externally. To facilitate this, the switch is meticulously configured, and static IP addresses are assigned to the servers. This strategic move not only improves data preservation but also reduces the risk of data loss, laying a solid foundation for the company's information infrastructure.

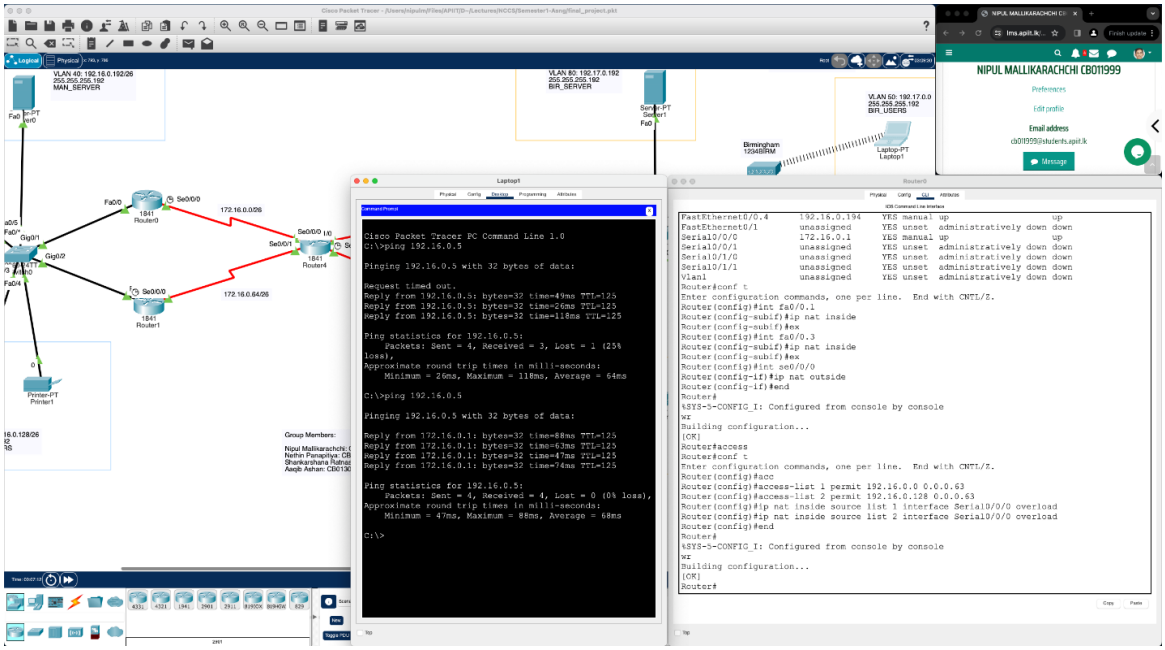


Figure 16

This illustrates the process of conducting ping tests to verify network connectivity. Pings that are successful are indicated by round-trip times in milliseconds, which are shown in white text on a blue background. The graphic also shows a representation of the router setup commands and outputs. IP address assignments and interface setups make up these parameters. When configuring a router to link an internal network (LAN) to an external network, such as the internet, the ip-nat inside command is utilised.All the private IP addresses that we are able to translate are included in the access list permit function, for example: access list 1 permit 192.16.0.0 0.0.0.63.It improves security by hiding internal IP addresses, conserves public IP addresses, and allows devices on a private network to connect to the internet without interruption.This configuration is visible throughout the router

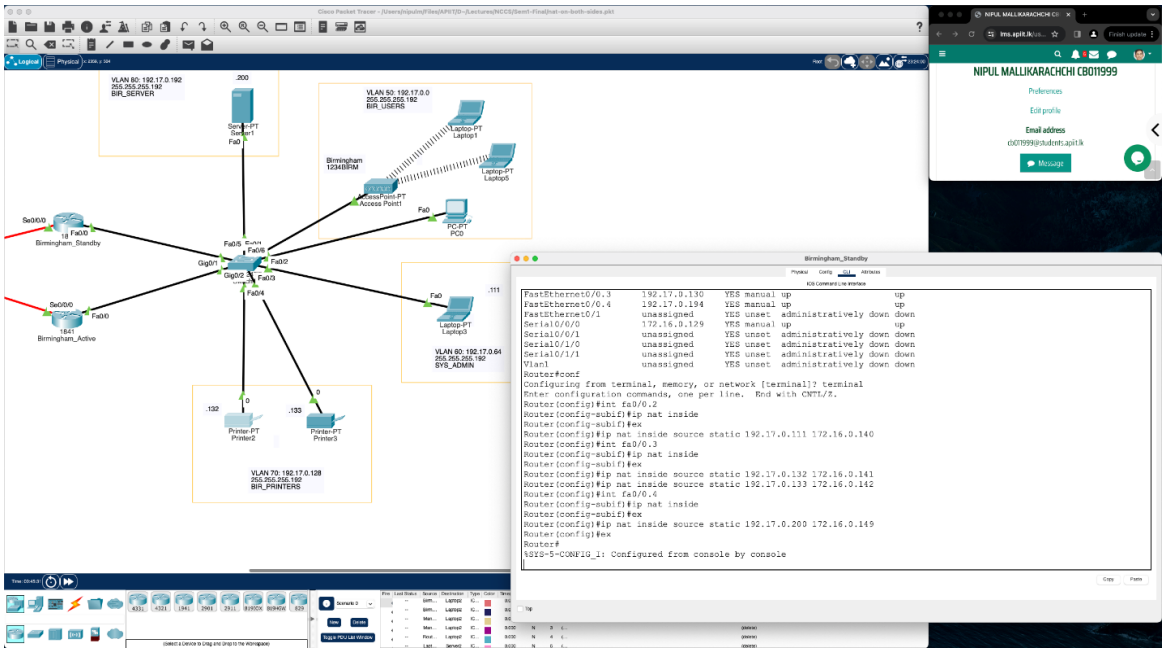


Figure 17

Using Network Address Translation (NAT) in the form of Protocol Address Translation (PAT), which enables the mapping of several local network devices to a single public IP address. Every internal private IP address has a unique port assigned to it, whereas a single public IP address is used for all of them. Within the source static function, IPNAT This section of the command defines a static translation between an inside global IP address, which is the IP address of that device as it appears to the outside world, and an inside local IP address, which is the IP address of a device on your local network. 192.17.0.11: This is the inside local IP address. It's the actual IP address of a device on your local network.

172.16.0.40: It's the IP address that the device at 192.17.0.111 will appear to have to the outside world.

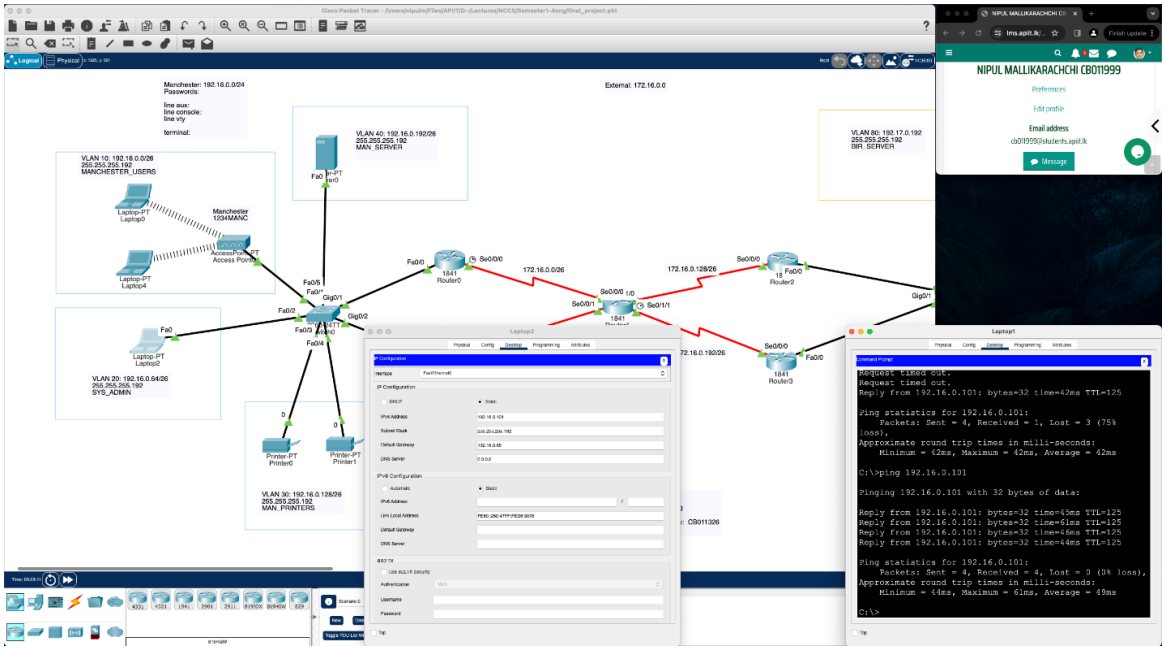


Figure 18

The laptop from Birmingham in this image is attempting to ping the laptop from Manchester (laptop 2) using its IP address, 192.16.0.101, which is shown in its IP configuration settings. Static connections have been employed as Because they are instantly locatable from anywhere in the globe and do not change like dynamic IP addresses, static IP addresses are perfect for running servers. They also offer greater reliability than dynamic IP addresses. Dynamic IPs can fluctuate often, occasionally resulting in connection losses. An additional line of defence against potential network security issues can be offered by static IP addresses. With a static IP address, various hardware and operating systems can connect to networks remotely.

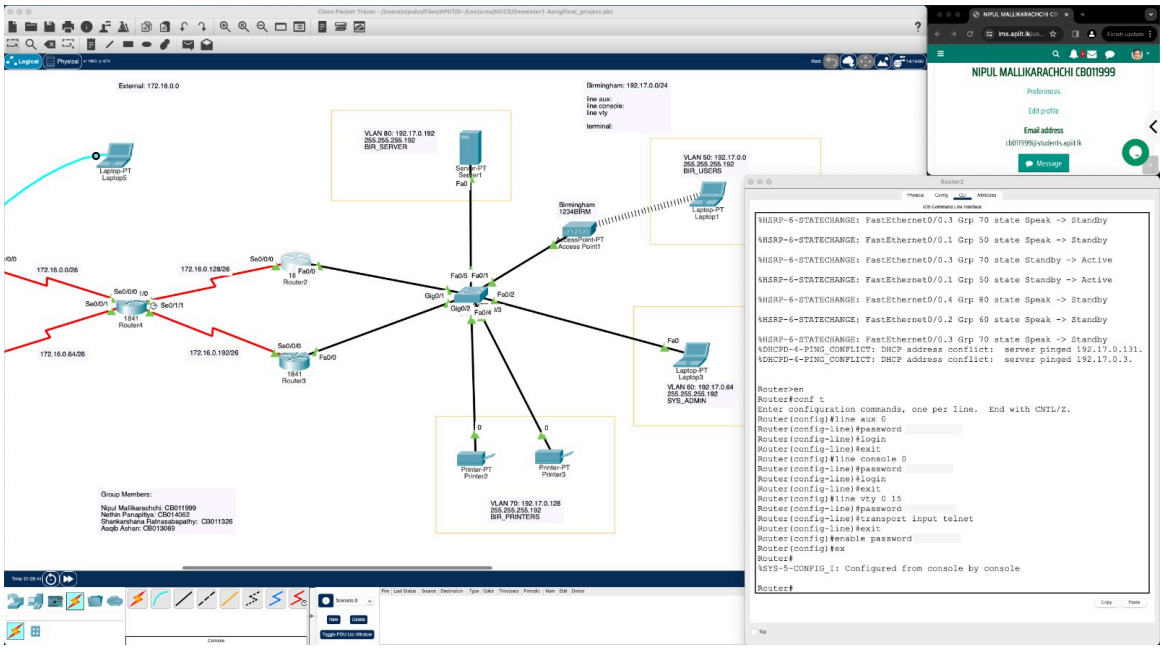


Figure 19

It is possible to examine the functions required to set the passwords on the relevant routers. The command "router(config)#PASSWORD" is used to set a password that must be supplied in order to gain access.

The real password needs to be entered in lieu of the placeholder. Router(config)#line vty 0 15: This command sets the VTY lines' configuration mode, which is necessary for remote router login.

Router(config-line)#login: This command is used to finish configuring the password and to enable password checking on the VTY lines. Additionally, it specifies the protocols that are allowed for incoming connections using (transport input telnet).

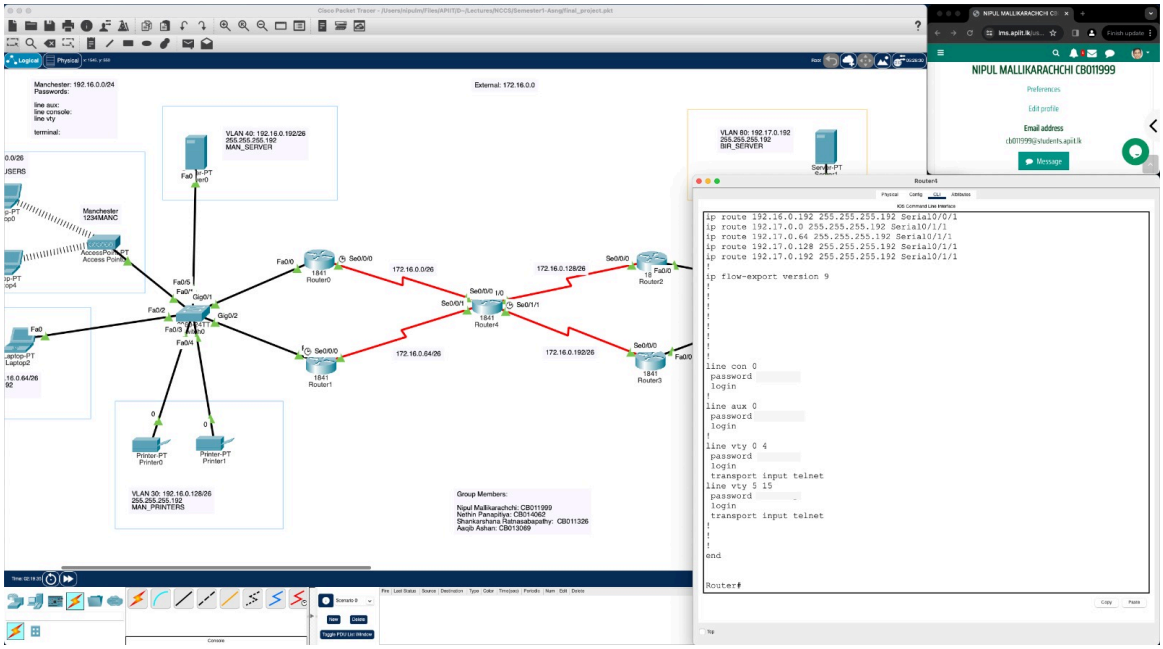


Figure 20

The console port is a physical port on the router or switch that allows you to locally manage the device. The command line con0 is used to enter the line configuration mode for the console port. The password command sets a password that must be entered to access the console port, and the login command enables password checking.
The auxiliary (AUX) port is typically used for out-of-band management of the router, such as configuring the device through a modem. The command line aux 0 is used to enter the line configuration mode for the AUX port. The password command sets a password that must be entered to access the AUX port, and the login command enables password checking.

Virtual Teletype (VTY) lines are used for remote access to the device, such as Telnet or SSH. The commands line vty 0 4 and line vty 5 15 are used to enter the line configuration mode for the VTY lines. The password command sets a password that must be entered to access the VTY lines, and the login command enables password checking. In conclusion, these commands are crucial for securing access to the network device. They allow you to set passwords for different types of access, ensuring that only authorized users can configure the device.

6. Device Connectivity and Access Control

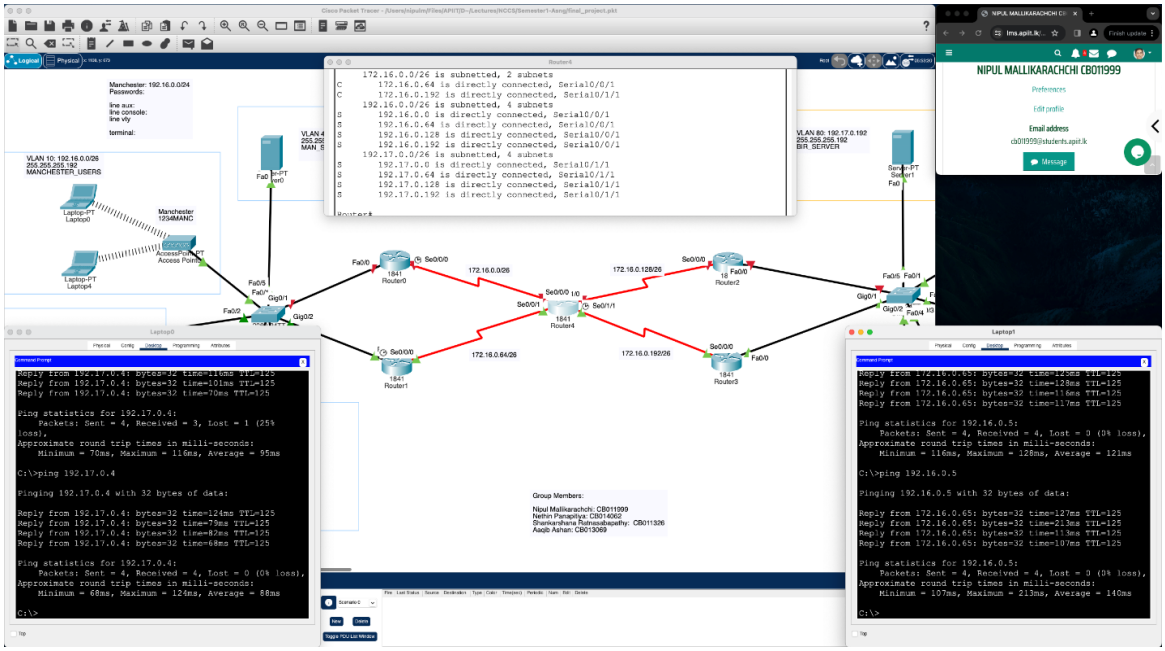


Figure 21

This image shows ip configs of router 4 which is basically the router that connects Birmingham and Manchester together and allows the users to send and receive information to the other city as well as from the city it shows that the internal ip addresses of Birmingham and Manchester (192.16.0.0/26 and 192.17.0.0/26) is subnetted into 4 subnets and are connected using the static method.

The validity of the configuration can be seen when trying to ping the laptops from Manchester and Birmingham and the statistics showing that all 4 packets have been received with 0% loss. This successful exchange of packets demonstrates the reliability and efficiency of the IP configurations on router 4. It ensures that users in Birmingham and Manchester can seamlessly communicate and share information, contributing to a smooth and uninterrupted flow of data between the two cities.

7. IP Addressing Scheme Overview (Table 3 & 4)

Subnet	Number of Hosts	Subnet Address	Subnet Mask	First Usable Address	Last Usable Address	Broadcast Address	No. of Unused IP Addresses
Manchester 1	64	192.16.0.0	255.255.255.192	192.16.0.1	192.16.0.62	192.16.0.63	30
Manchester 2	64	192.16.0.64	255.255.255.192	192.16.0.65	192.16.0.126	192.16.0.127	30
Manchester 3	64	192.16.0.128	255.255.255.192	192.16.0.129	192.16.0.190	192.16.0.191	30
Manchester 4	64	192.16.0.192	255.255.255.192	192.16.0.193	192.16.0.254	192.16.0.255	30

Figure 22

This is the summery of the Manchester IPS giving the subnet mask the subnet address and other important stuff.

Subnet	Number of Hosts	Subnet Address	Subnet Mask	First Usable Address	Last Usable Address	Broadcast Address	No. of Unused IP Addresses
Birmingham 1	64	192.17.0.0	255.255.255.192	192.17.0.1	192.17.0.62	192.17.0.63	30
Birmingham 2	64	192.17.0.64	255.255.255.192	192.17.0.65	192.17.0.126	192.17.0.127	30
Birmingham 3	64	192.17.0.128	255.255.255.192	192.17.0.129	192.17.0.190	192.17.0.191	30
Birmingham 4	64	192.17.0.192	255.255.255.192	192.17.0.193	192.17.0.254	192.17.0.255	30

Figure 23

This is the summery of the Birmingham IPS giving the subnet mask the subnet address and other important stuff.

The routing table includes devices named "Manchester 1" through " 4", "External 1" through "5", and "Birmingham 1" through "4". Each device has a unique IP address, subnet mask, and default gateway. The subnet mask defines the subnet that the device is on. The default gateway is the router that the device will use to send traffic to other networks.

Host/Device/Interface	IP address Start	Mask	Default Gateway	DCE/DTE
Manchester 1	192.16.0.0	255.255.255.192	192.16.0.1	Manchester
Manchester 2	192.16.0.64	255.255.255.192	192.16.0.65	Manchester
Manchester 3	192.16.0.128	255.255.255.192	192.16.0.129	Manchester
Manchester 4	192.16.0.192	255.255.255.192	192.16.0.193	Manchester
External 1	172.16.0.32	255.255.255.224	172.16.0.33	External
External 2	172.16.0.64	255.255.255.224	172.16.0.65	External
External 3	172.16.0.96	255.255.255.224	172.16.0.97	External
External 4	172.16.0.128	255.255.255.224	172.16.0.129	External
External 5	172.16.0.160	255.255.255.224	172.16.0.161	External
Birmingham 1	192.17.0.0	255.255.255.192	192.17.0.1	Birmingham
Birmingham 2	192.17.0.64	255.255.255.192	192.17.0.193	Birmingham
Birmingham 3	192.17.0.128	255.255.255.192	192.17.0.129	Birmingham
Birmingham 4	192.17.0.192	255.255.255.192	192.17.0.193	Birmingham

Figure 24

8. Estimated Cost Analysis

The estimated cost for setting up the network infrastructure includes equipment, installation, connectivity, maintenance, and miscellaneous expenses. Equipment costs involve routers, switches, wireless access points, cloud servers, a sys-admin machine, and printers. Installation and configuration encompass labor costs, DHCP server setup, server farm migration, and VLAN configuration. Connectivity costs include upgrading the DSL link and ISP subscription fees. Ongoing maintenance entails cloud service subscriptions, support contracts, and staff training. Miscellaneous expenses cover cabling, power backup, and security tools. While the exact cost varies based on vendor pricing and specific requirements, a rough estimate for a similar setup is approximately $5500 USD, based on analysis of comparable small business networks.