Name: Daniel Cyril Obon

Student ID: C2650218

1. Diagram of Network Design

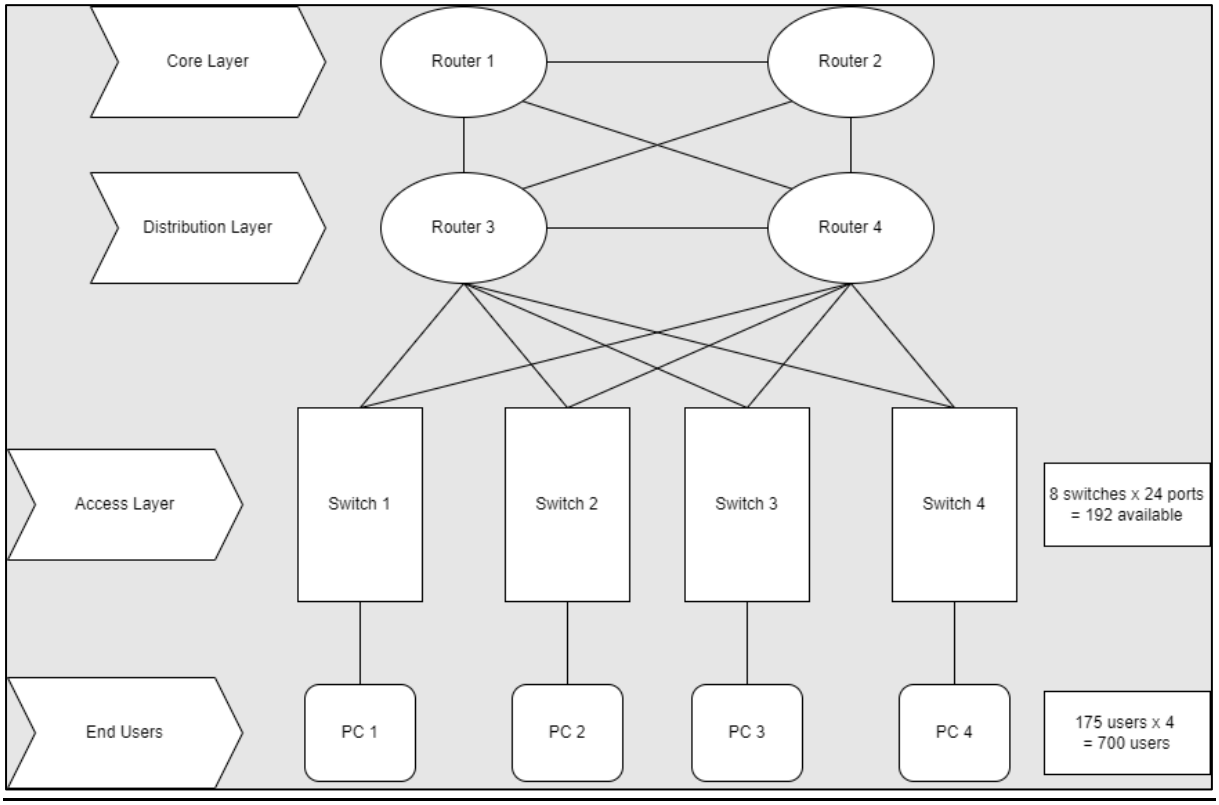

Figure 1.0: Full Network Diagram

2. Network in Packet Tracer

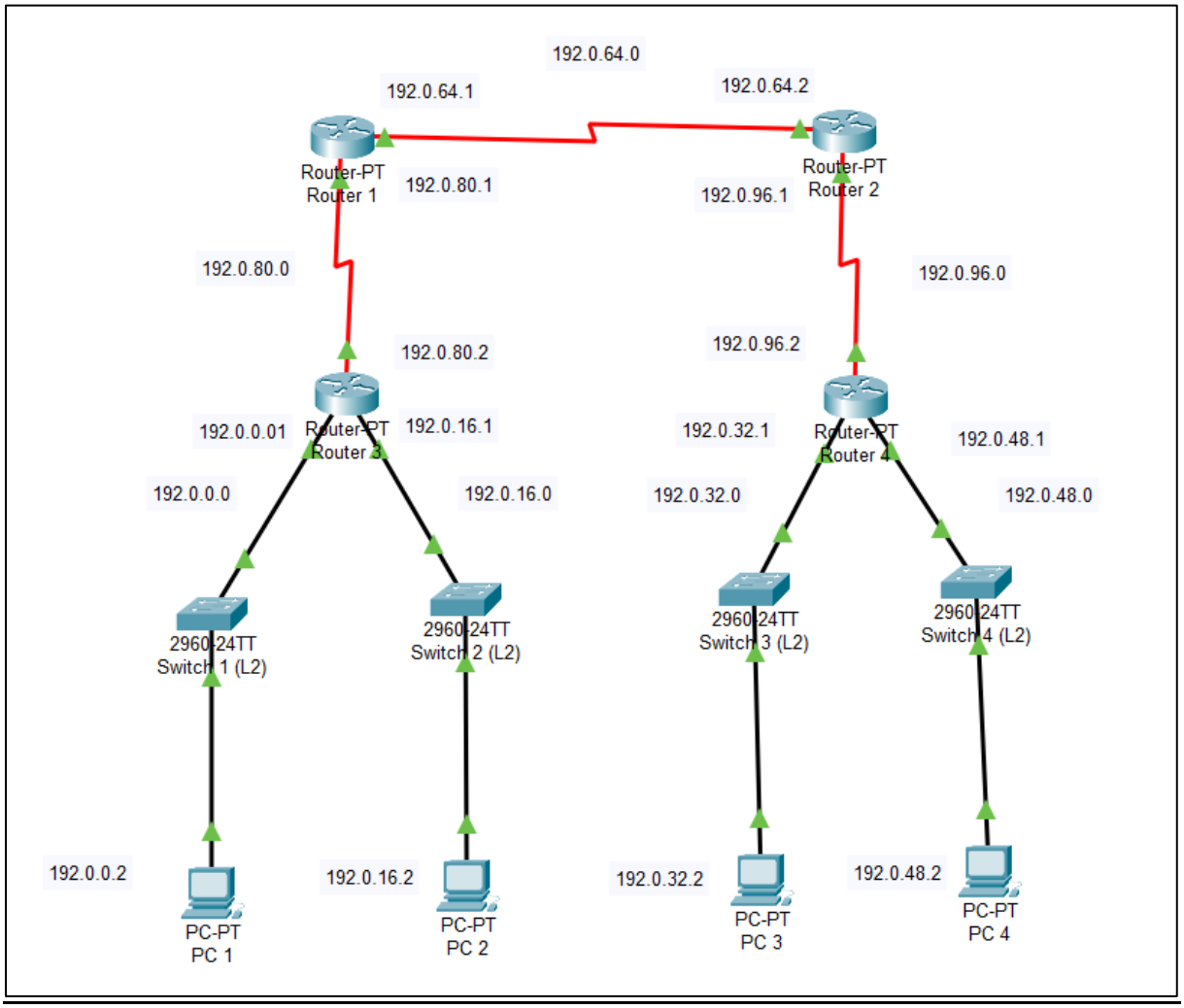

Figure 2.0: Implemented Network Design (Simplified)

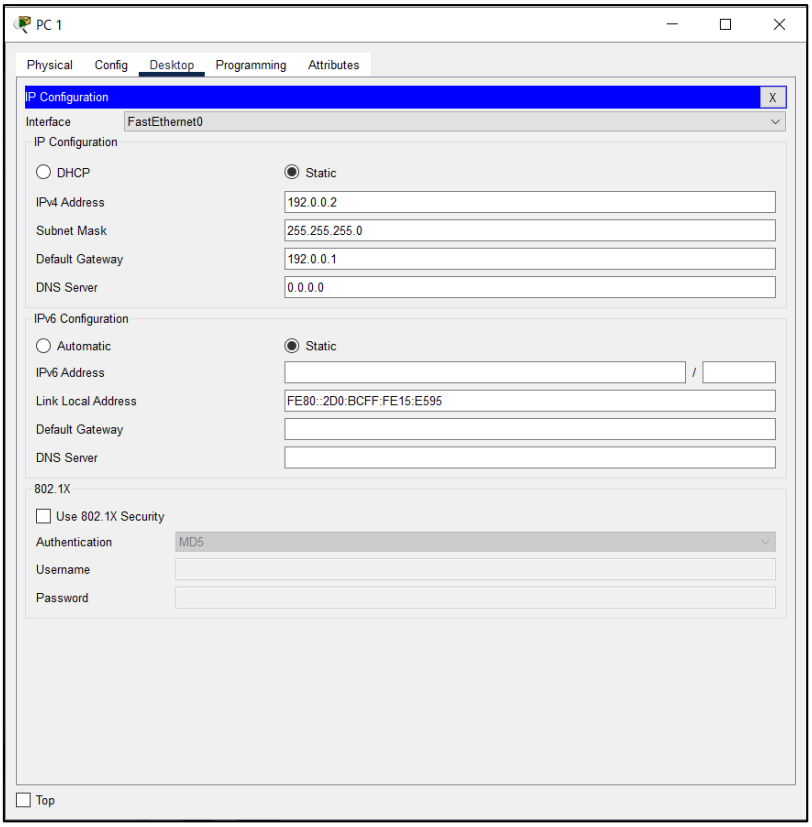

Figure 2.1: PC Configuration

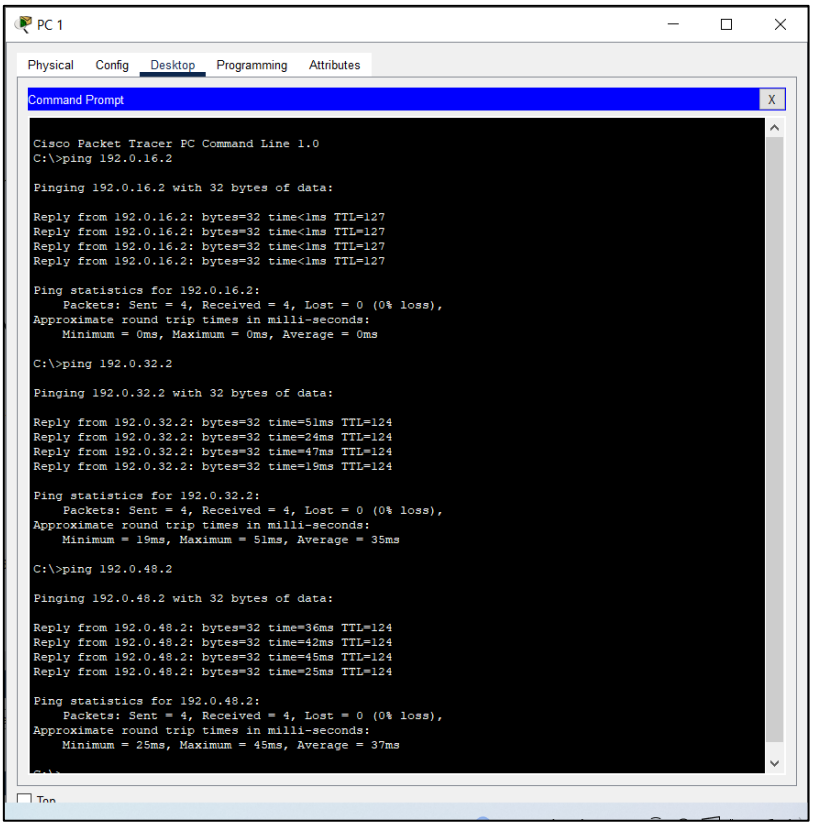

Figure 2.2: Pinging PC

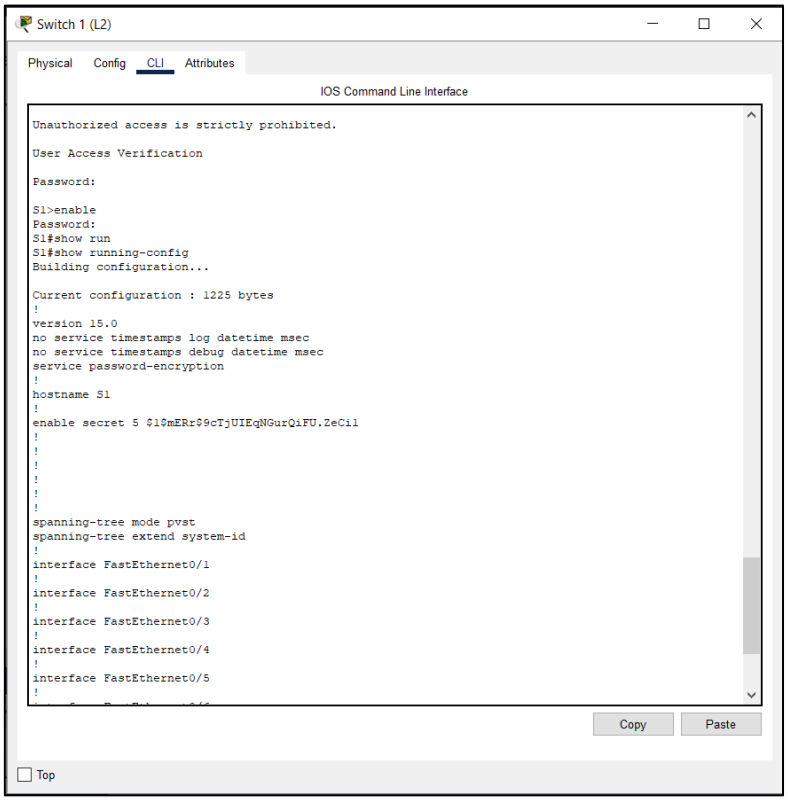

Figure 2.3: Secret Password Security Implementation on Layer 2 Switch

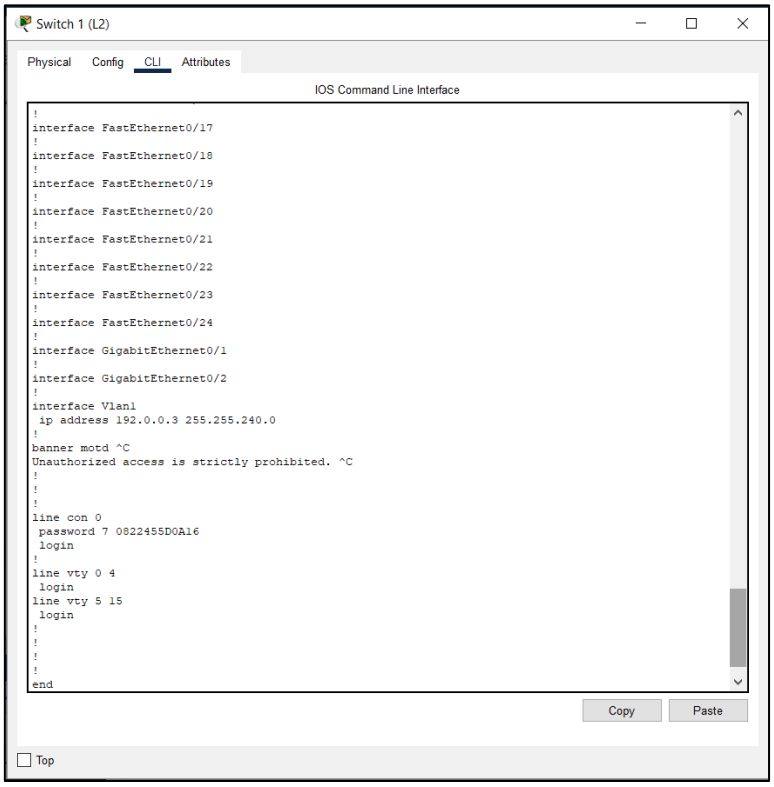

Figure 2.4: Console and Banner MOTD Implementation on Layer 2 Switch

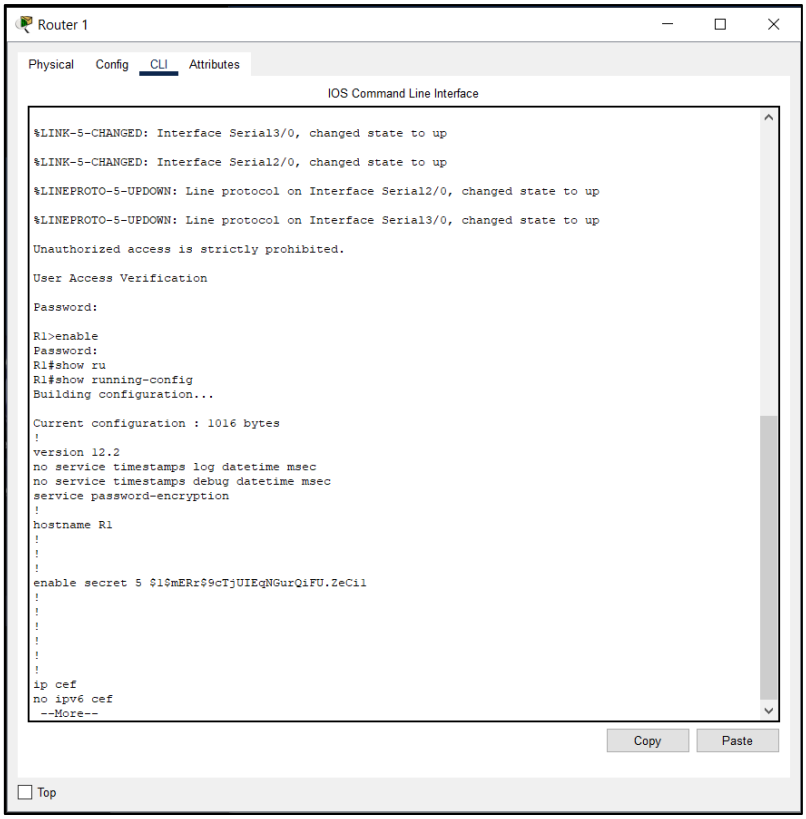

Figure 2.5: Secret Password Security Implementation on Layer 4 Router

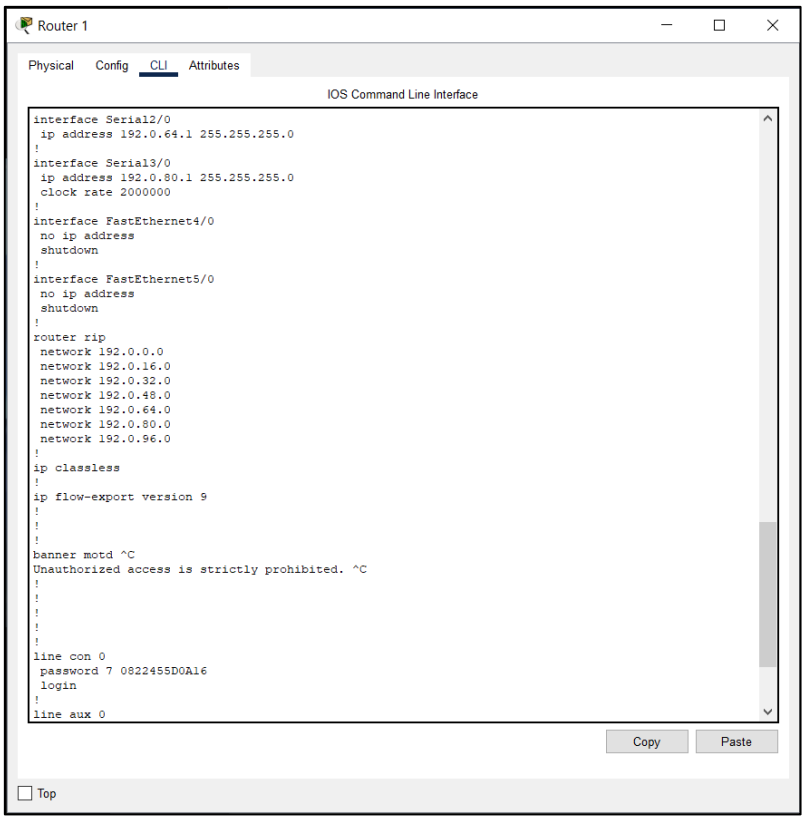

Figure 2.6: RIP, Console and Banner MOTD Implementation on Layer 4 Router

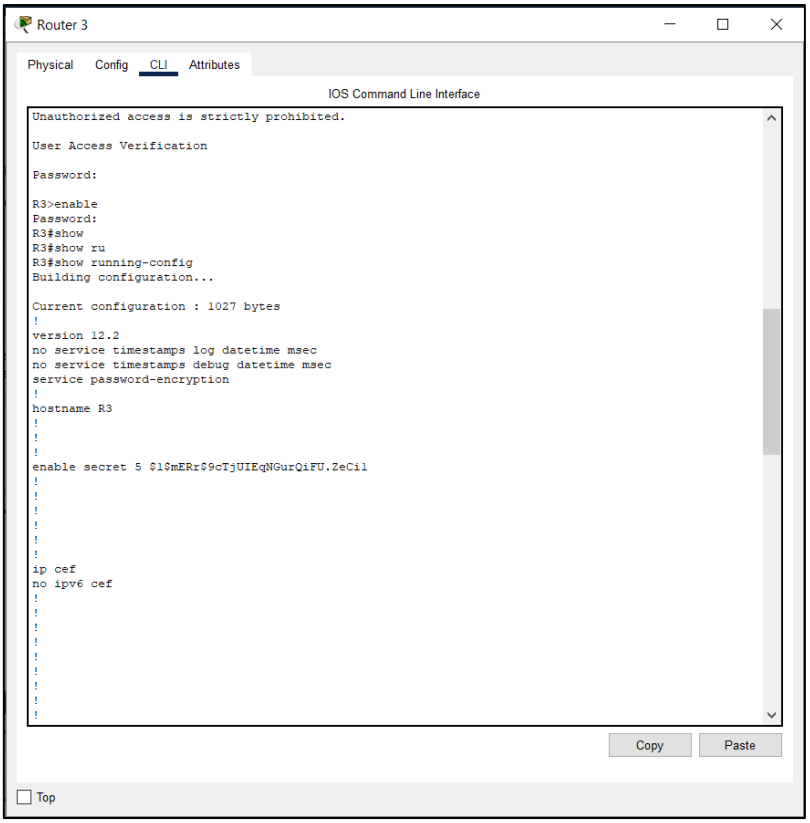

Figure 2.7: Secret Password Security Implementation on Layer 3 Router

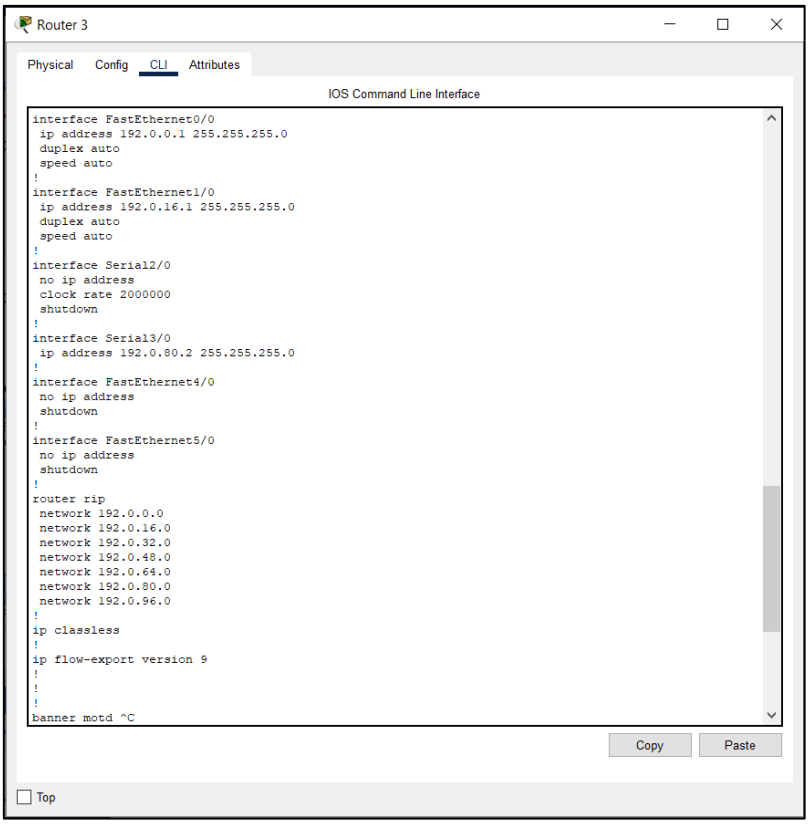

Figure 2.8: RIP, Console and Banner MOTD Implementation on Layer 4 Router

3. Proposed Subnet Solution

Table 1: Binary to Decimal

128	64	32	16	8	4	2	1
1	1	1	1	0	0	0	0

Table 2: Number of Users to Bits

Bits	1	2	3	4	5	6	7	8	9	10
Host	2	4	8	16	32	64	128	256	512	1024

Subnets: 10 (700 users)

Class: B

Default Subnet Mask: 255.255.0.0

Zero in Mask to Binary: 00000000 00000000

Requirements: 11110000 00000000

Convert New Mask to Decimal: 240 0

Subnet Mask: 255.255.240.0

Subnet ID	First Useable IP	Last Useable IP	Broadcast Address
192.0.0.0	192.0.0.1	192.0.17.254	192.0.17.255
192.0.18.0	192.0.18.1	192.0.31.254	192.0.31.255
192.0.32.0	192.0.32.1	192.0.47.254	192.0.47.255
192.0.48.0	192.0.48.1	192.0.63.254	192.0.63.255
192.0.64.0	192.0.64.1	192.0.79.254	192.0.79.255
192.0.80.0	192.0.80.1	192.0.95.254	192.0.95.255
192.0.96.0	192.0.96.1	192.0.111.254	192.0.111.255

4. Report

4.1 Design Developed for Scenario

For this scenario the network layout in Figure 1.0 is used, and a simplified version of the network is implemented in Cisco Packet Tracer. For Layer 4 (Core Layer) two routers, called Router 1 and Router 2 are set up. For Layer 3 (Distribution Layer) another two routers, called Router 3 and Router 4 are set up. These four routers are then connected in a full mesh spanning tree protocol (STP). The purpose of doing so is to prevent a single point of failure that would have been faced when using only one router/ISP, which is also a similar why the Distribution Layer is set up as such.

Besides that, a router is used in the instead of a Layer 3 Switch due to it providing better security for the network, where these switches are connected to the routers in Layer 4 (Distribution Layer) using copper cables (such as CAT 5e). This is due to its better ability in sorting traffic such as by ports, protocols or IP addresses destination. Moreover, a router also is more scalable and flexible than switches which in turn helps in its futureproofing. For the benefits in scalability, this can be attributed to the fact that routers can support more traffic and devices which leads to it being expandable. As for flexibility, this is because routers support more network protocols as well as types of networks. Lastly, it allows for more redundancy in pathing due to meshing for a network which increases the network availability thus making it more reliable due to its lower downtime.

In addition, routing information protocol (RIP) is also implemented between the four routers in Layer 4 (Core Layer) and 3 (Distribution Layer) which is used for connecting the routers together by the exchanging of routing information. This can be seen in the implementation from Cisco Packet Tracer in Figure 2.6 and Figure 2.8. Another benefit of RIP is due to its ease in implementation. Moreover, other forms of security such as passwords and encryption which can been seen in Figure 2.5 and Figure 2.7 are also implemented on both the switches and routers respectively. Doing so increases the security of the network and ensures that unauthorised access is lessen to a degree.

For Layer 2 (Access Layer), four stacks of eight switches are used, then each switch stack is connected to both Router 3 and Router 4 in Layer 3 (Distribution Layer), where these Layer 2 switches are then connected to the users through a copper cable. A The reason for doing this is due to pathing redundancy which helps in minimising the downtime of the network. There are four subnets in this network, where each switch is responsible for a subnet that is also expandable in the future. Due to each stack of switches having eight switches, the total number of users supported for the current stack is 192 per stack. However, for this network design only 175 users will be used for each switch stack. This makes it a total of exactly 700 users being supported for this network design. This benefit also extends in helping maintain the network as less users will be affected due to the separated subnets. The extra/additional subnets that have not been used for the network design could be used in the future for expansion when adding more subnets and users.

4.2 Security Issues Identified with the Processes and Policies Used to Mitigate the Risk

A security issue that could be noticed is from the full mesh topology that is implemented in the network design. With full mesh topology, it leads to more redundant network connections in the design and thus more areas for attackers to invade. Besides that, a full mesh topology also has an increased complexity of design which in turn could make it more challenging to manage the security of the network.

Another security flaw could be due the implementation of (Routing Information Protocol) RIP as well as the use of Layer 3 (Distribution Layer) Router instead of Layer 3 Switch. Some drawbacks that come with the implementation of RIP such as its vulnerability to spoofing as well as traffic attacks. These are due to the multiple redundant pathing made in the network, which as mentioned previously, leads security risk. Moreover, RIP does not provide a way to authenticate routing information which may lead to traffic attacks/interception due to spoofing in the network.

Some ways to mitigate these problems is to implement security features such as intrusion detection systems (IDS) and firewalls which will help in treat prevention. Firewalls can act as access control which could restrict the traffic between certain network connections, and thus also works alongside IDS which helps in detecting unauthorised network connections. Encryption can also in this endeavour as it helps in encoding the data in the network so that it will be more difficult for attackers to decode the data without the help of a decryption key.

Besides that, network segmentation is another method to combat these security issues. These can be implemented by using Virtual Local Area Networks (VLAN) to differentiate subnets into different segments which separates the network traffic and thus increases the network security by minimising security breaches affecting the whole network.

Moreover, security maintenance and testing should also be done regular for the network. Checking and testing the network on a regular basis is essential in its upkeep as it helps in identifying any network vulnerabilities during testing which in turn keeps the network up to date in terms of security, increasing the networks security.

4.3 Ethical and Legal Issues to be Considered in Network Design and Management

A factor that should be taken into account when considering the ethical and legal issues of network design and its management is the privacy it provides to the users of the networks. With the Data Protection Act 2018 implemented by the GDPR in the UK, it states the personal data that is collected can only be used lawfully and transparently. With the enactment of this act, it allows for users to request data on how or what their data is being used for. As such, this gives users of the network more peace of mind of the use of their personal data. In addition, the Computer Misuse Act 1990 also helps in this predicament as it bolsters data protection by ensuring only authorised use of computer systems when handling data. It also covers the misuse of malware by making it against the law to create or spread them.

Network security is also another factor to consider for network design and management. If a network has subpar network security implementation, it could lead to legal action being taken against the owner of said network. With weak network security, it could lead to data leaks which can come with a very heavy penalty. Under the Data Protection Act, a company in breach of this will be fined £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher. With this in place, it incentivises company to invest resources in having a secure network as to not breach said act.

Another consideration is the ethical use of networks in the workplace, be it a company or an individual. Companies should hold and promote workshops or seminars on the ethical use of networks yearly as to teach and remind employees on the importance of enforcing policies in networks as well as discourage them from doing anything that could harm others and will go against any laws and acts that are enacted. This could also extend to having regular monitoring and testing of networks as to ensure that said network is up to par and is within the law and industry standard.

4.4 Reflection on Solution

The network proposed in Figure 1.0 has met most of the business requirements as it supports the 700 users that is requested by using Class B subnetting. Due to using Class B subnetting, these 700 users could be further increased in the future as the network design is flexible and scalable. This can be done by stacking more switches and/or creating more subnets within the network to support more users, leading to its futureproofing.

Besides that, main routing protocol RIPv1 has also been implemented in the network design. This can be observed in Figure 2.6 and Figure 2.8 for the Core Layer routers and Distribution Layer routers respectively. RIP is implemented by giving the reserved IANA IPv4 addresses for each subnet to the routers. By implementing this, the network is able to share information between routers thus connecting the switches and users from different subnets. Moreover, CAT 5e cables are also used to connect the networks in the physical layer.

Another requirement that is achieved is the use of spanning tree in the network. As seen in Figure 1.0, a full mesh topology is used to connect the routers in the Core and Distribution Layer. As mentioned previously in the report, the implementation of full mesh helps in minimising the downtime of networks as it prevents single points of failure if full mesh is not implemented, thus making a more reliable network design.

A subnet of class-based IPv4 is also used in the network design, which fulfils one of the business requirements. With this implementation, Class B subnetting is used for the implementation to support the number of users required. For class B with 8 subnets, the subnet mask 255.255.240.0 is used for the machines and networks connecting them together.

However, a requirement that was not met is the 15-character password used for authentication in key network services. Though the requirement is not demonstrated in the implementation as it was using a 5-character password, this can easily be changed by going into the terminal configuration of the routers and switches and change them into a 15-character one.

Overall, though the network is not implemented exactly to the requirements, most of it has been satisfied. Moreover, the 5-character password that was wrongly implemented in Cisco Packet Tracer can be changed, provided that the previous passwords are known to access the switches and routers.