**COMP40002**

**Networking Concepts and Cyber-Security: Case Study**

Prepared by

Jamie Carson

John Volosenco

Jack Riley

A red and grey logo

Description automatically generated

**Contents**

**1. Internal IP Addressing Scheme**

1.1 IP Addressing Scheme:

1.2 DHCP Implementation for Both Sites

**2. IP Addresses for Inter-site Link**

2.1 Determining IP Addresses for the Link

2.2 Ensuring Scalability for Future Growth

**3. Benefits and Requirements of Virtual Local Area Networks**

3.1 Virtual Local Area Network advantages

3.2 Meeting Network Traffic Management Needs

3.3 Improving Security through VLANs

**4. WAN Connections Requirements**

4.1 Connection Points for WAN

4.2 Throughput Requirements for Efficient Communication

4.3 Available WAN Technologies

4.4 Benefits and Risks Associated with Selected WAN Technologies

4.5 Implementing WAN Link Redundancy

4.6 Estimated Cost Analysis

**5. Justification for Device and User Selection**

5.1 Choice of Networking Devices

**6. Security Implementation**

6.1 Enhancing Security Measures in Manchester

6.2 Appropriate Security Measures in Liverpool

6.3 Addressing External Access and Ensuring Sys-Admin Security

**Introduction:**

A small company located in Manchester is currently developing its internal infrastructure and expanding its operations. With plans to open a new branch in Liverpool and hire more staff, the company aims to update and replace their antiquated systems. Nevertheless, they face constraints with their existing internet connection—a sluggish and erratic 20 Mbps Digital Subscriber Line (DSL) link to the Internet service provider (ISP). Therefore, the business needs a comprehensive network update. This report will outline suggested fixes and provide supporting arguments to address the company's urgent network needs successfully.

**Synopsis:**

The company's expansion strategy involves upgrading the infrastructure in Manchester, establishing a new site in Liverpool, and ensuring seamless connectivity between both locations. Key goals include setting up distinct internal Internet Protocol addresses (IP address), establishing redundant network connections to maintain business continuity should any primary network connections fail, bolstering security protocols, and relocating servers to Liverpool to create an internal private cloud system.

1. **Internal IP Addressing Scheme**

**1.1 IP Addressing Scheme**

The project will primarily require a classless subnetting scheme since only a class C subnet from the internet service provider is available for each site.

A class C subnet would provide 254 IP addresses and only one subnet. Using a classless IP addressing scheme is more efficient for several reasons. Steve Petryschuk documents this in an article explaining the limitations of a classful addressing scheme include being unable to designate small amounts of IP addresses to a subnet1. For example, if we only needed 50 IP addresses for a subnet, we would be wasting 204 IP addresses.

The solution to this is using Classless Inter-Domian Routing or CIDR. Classless addressing enables networks to be decoupled from default subnet masks. In contrast, we had only 254 addresses to use on a class C network; it is now possible to divide that subnet into smaller subnets, allowing the segmentation of blocks of IP addresses. This allows networks to efficiently assign a range of IP addresses without wasting a significant number of IP addresses that can be utilised elsewhere on the network.

Alternatively, the project could have one extensive Class C network for each site. However, this could cause various security issues. All departments would have access to any network traffic, with the site requiring four different departments (Administration, Office, Wireless access and a Server farm); this could be a security flaw. Dividing the singular network into multiple, smaller subnets reduces the risk of sensitive data being broadcast to other departments. Dividing the network into smaller subnets is known as Variable-Length Subnet Masking (VLSM) and is an efficient protocol to utilise IP addresses.

**1.2 DHCP Implementation for Both Sites**

There is also a requirement for Dynamic Host Configuration Protocol or ‘DHCP’ for both sites, which issues IP addresses automatically via a server rather than having manually assigned IP addresses (static addresses). The server is given a range of IP addresses assigned to hosts on request. This protocol limits the scenario of having two devices with the same IP address, which causes network errors. Their other significant advantage is that IP addresses are managed at one point, reducing the need for in-depth configuration on different hosts, which may require personnel to be onsite to action.

There are risks associated with DHCP; if the server is down for any reason, any hosts using DHCP will not have any connectivity; specific devices also do not support DHCP. These are unlikely events but still a possibility.

The decision to still use static IP addresses for specific devices such as servers and network printers is still viable as the likelihood of these devices requiring a different IP address is unlikely to occur. Having one IP address for these devices is advantageous so hosts such as desktop computers and laptops know precisely where to find them.

**2. IP Addresses for Inter-site Link**

**2.1 Determining IP Addresses for the Link**

Due to the distance between the two sites, a point-to-point link is not a cost-effective, viable option; instead, a set-up with two external-facing routers connecting the two sites through an ISP would be more beneficial. The external routers for each site use connections via gigabit ethernet ports with 1000 Mbps, increasing bandwidth by 4900% per router and adding redundancy if one router fails.

Using the external IP address provided by the ISP, which again will be a class C address, subnetting this into smaller blocks of IP addresses. This gives two available addresses for each router, a start point and an endpoint, increasing efficiency due to the fact that there is less routing information on the subnet., reducing IP wastage and increasing security as there are fewer IP addresses that could be compromised.

**2.2 Ensuring Scalability for Future Growth**

The mentioned actions also contribute to future-proofing the network, facilitating growth and scalability for additional sites to be added and implementing VLSM on routers and switches to reduce IP address wastage.

Furthermore, the network will exclusively use Cisco devices employing a proprietary routing protocol, Enhanced Interior Gateway Protocol (EIGRP). EIGRP enables fast and efficient routing by autonomously identifying and adapting to any network fluctuations or alterations on the network2. It uses the Diffusing Update Algorithm to calculate the most optimal path to read its next destination. EIGRP enables additional routing equipment to be introduced into the network with minimal configuration.

The following tables illustrate how the network utilises subnetting (Fig 1 and Fig 3.), while a list of IP addresses assigned to each host or interface is provided in Fig 2 and Fig 4.

**Manchester Ip Address Ranges**



Figure 1:

Figure 2:

 **Liverpool IP Address Ranges**

Figure 3:

Figure 4:

**3. Benefits and Requirements of Virtual Local Area Networks:**

**3.1 Virtual Local Area Networks advantages**

Before discussing the advantages of using segmentation within Virtual Local Area Networks (VLANs)5, it is essential to understand them. According to Mike Petryschuk, “A VLAN shares similar characteristics to a LAN, but a VLAN allows different computers and devices to be connected virtually to each other as if they were in a LAN sharing a single broadcast domain”3.

Mike Petryschuk also demonstrates the use of VLANs with a simple diagram showing that even though the devices are connected physically to the same switch, the devices are segmented into different VLANs, only allowing the specific VLAN to broadcast without any traffic being leaked to other departments.

A diagram of a computer network

Description automatically generated

Figure 5:3

There are various advantages, some of which we will explain further in the next section, but a big factor is cost and simple IT management. Managing virtual networks without physical devices to segment the network and with less requirement for IT support to be on site as the administration of such technology can all be done remotely.

**3.2 Network Traffic Management Needs**

With one of the critical requirements of the Manchester site being improved speed and efficiency, using VLAN presents a positive solution: reduced broadcast traffic on the network. As the various departments would be separated into their own VLAN, any traffic from servers, office computers, and internal or external Wi-Fi connections would no longer flood the network, causing potential slowdown.

The naming convention for the VLANs follows a digital format for the VLAN interface, from 0 to 4096, with the ability to name each VLAN interface up to 15 characters. The Manchester site will be required to have five separate VLANs, which can be seen in Fig 6.



Figure 6:

The Liverpool office will follow the same format, excluding the Guest Wi-Fi, as there is no requirement at the time of this report. This naming format allows system administrators to make changes to individual VLANs without checking which VLAN is for which department.

There is also the ability to implement Quality of Service to different VLANs and set priorities for certain types of traffic. There may be a requirement for the office hosts to have priority to high-bandwidth video traffic, such as using Microsoft Teams or any other video-conferencing application. Increased flexibility and scalability also present an advantage when using VLAN technology, adding or removing departments and creating new departments, which can all be done remotely and with little or no change to the physical infrastructure, facilitating network growth for any business size.

**3.3 Improving Security through VLANs**

An important consideration is how security could be improved at the Manchester site and implemented at the new Liverpool site.

VLANs offer a robust, secure infrastructure; in the network design, layer three routing technology Switches are used to communicate between the different VLANs. This configuration ensures that traffic only intended for a specific host or sub-network is not flooded to all the other subnets. A good example is the requirement for the Manchester site to have internal and guest Wi-Fi. Having these two networks on separate VLANs ensures that any internal traffic is not accessible by any device using the Guest Wi-Fi, ensuring sensitive company data is isolated from any external access.

1. **Wide Area Networks (WAN) Connections Requirements:**

**4.1 Connection Points for WAN**

Deciding what connection points will need to access the wide area network is vital when looking at which WAN technology needs to be incorporated to link local area networks together. In this scenario, the main concerns are connecting Branch offices and remote users for both sites. There is also connectivity to a private cloud for the Liverpool site that needs to be considered. The connection points will be provided physically by two routers for each site.

**4.2 Throughput Requirements for Efficient Communication**

Several factors need to be outlined when deciding the throughput requirements to ensure efficient communication.

* + - 1. Identify devices and device requirements.
      2. Understand what applications will be used: video conferencing, software development applications, and file servers.
      3. Total connections at peak times
      4. What redundancies will be in place on the network?

For the design of both the Manchester and Liverpool sites, the following can be estimated for a peak time value: -



Figure 7:

This would give a maximum throughput of 1000mbps. Looking at the Network design, this would be achievable as two routers using gigabit ethernet ports can handle 1000mbps each, giving a total of 2000mbps and adding redundancy and disaster recovery.

**4.3 Available WAN Technologies**

There are many options for which WAN technology to implement within a network. Here is a list of some popular options embraced by businesses.

**MPLS (Multiprotocol Label Switching)**

A reliable WAN technology that offers mostly guaranteed connection and quality of service support.

**SD-WAN (Software-Defined Wide Area Network)**

SD-WANs have been gaining popularity with present-day businesses for their ease of use, flexibility, and low cost.

**Leased lines**

A dedicated point-to-point connection is solely used by the organisation that leases the line. These are usually offered at a fixed rate regardless of how much bandwidth is used, making them less cost-effective in fluctuating business environments.

**4.4 Benefits and Risks Associated with Selected WAN Technologies**

Looking at a cost-effective solution to connect the Manchester site and the Liverpool site while still maintaining efficient network communication meant a point-to-point link would not be viable due to the distance between the two sites.

A more cost-effective option will be a Software-Defined Wide Area Network or SD-WAN. An SD-WAN works by using a connection to an ISP to use a virtualised service; if any LANs have an internet connection, they can be linked to form a Wide area network.

More and more businesses are opting for using an SD-WAN rather than the more traditional WAN for several reasons: -

1. Secure connectivity – all traffic is encrypted.
2. Load balancing – connections that adapt to unstable network conditions.
3. Ease of use – Ability to change configurations instantly and remotely.

However, there are some disadvantages with SD-WANs.

1. Most SD-WANs are done over the public internet, which eliminates end-to-end Quality of Service.
2. As access is cloud-based, there is no onsite security; organisations must be responsible.
3. SD-WANs: The software tends to be self-service, which may mean additional IT support or costs to bring in a third party to configure environments.

**4.5 Implementing WAN Link Redundancy**

An SD-WAN will also provide redundancy by rerouting network traffic to ensure constant and consistent data flow between points.

AT&T explain how they provide redundancy using their SD-WAN package, stating that if networks experience unplanned downtime or periods of heavy traffic, the network will adapt autonomously through software, making SD-WANs an excellent choice for large or small business networks4.

**4.6 Estimated Cost Analysis**

The following information outlines the anticipated expenses for the necessary equipment and technology. There may be an option to use existing equipment, which should be considered.

Figure 8:

**5. Justification for Device and User Selection:**

**5.1 Choice of Networking Devices**

This network design will use a range of devices to handle the VLAN segmentation effectively. Layer 2 switches will act as a physical host to pass network traffic from each VLAN via an access link; this is then passed through trunk links onto a multilayer switch that operates on both layer 2 and layer 3 protocols of the OSI model. The Layer 3 switch is responsible for routing the traffic to the correct destination, whether out to an external network or internally to a separate VLAN. With this IP routing, the VLANs can communicate with each other.

As redundancy is always a consideration in any part of a network to ensure business continuity, a second Layer 3 switch will connect to each of the layer 2 switches handling the VLANs. This Layer 3 switch will act as a standby should anything happen to the active Layer 3r switch; this standby device will take control. For this to happen, Hot Standby Router Protocol (HSRP) is implemented on both active and standby switches. HSRP works by assigning a device a priority over the secondary device; all traffic will be routed to the primary device until there is an issue where the secondary device will take control of the data flow. This protocol also allows the Active router to take back control once back online, ensuring that the Primary Switch is always active wherever possible.

Another advantage of using Layer 3 switches for handling data flow is that the devices automatically configure Spanning Tree Protocol (STP). Wherever any layer 2 devices are linked in a loop, it can cause severe problems for a network as these can become infinite network loops, flooding the network with unnecessary traffic; in severe cases, network flooding can bring a network down. STP combats this by blocking a connection to break the loop, only unblocking if that path is required due to a fault on other lines.

A diagram of a network

Description automatically generatedFinally, two routers face the external network above the Layer 3 switches. Having these routers in play allows for redundancy; should one router fail, there is still a router for traffic to be routed. The other reason is that under peak times of the business, the additional device improves network throughput, allowing more significant amounts of data to be sent out of the internal network. Figure 9 illustrates how the completed network may look.

Figure 9:

**6. Security Implementation:**

**6.1 Enhancing Security Measures in Manchester**

Security measures will be implemented to ensure each device has multiple measures in place. A defence in Depth approach ensures that any attempt for malicious access is met with multiple defences. Ensuring the business employs security policies such as securing host devices and using secure passwords with strict guidelines on how this should be achieved can prevent most unwanted access events.

Each network device will require a username and password to access the system and a further password to enter privileged EXEC mode—a message banner on each device to warn that unauthorised access is prohibited. Password encryption will also be applied to convert plain text passwords into encrypted Hash using the message Digest Algorithm (MD5). Devices will also implement the Authentication, Authorisation and Accounting services to control user access, log user activities, and restrict unauthorised commands.

Finally, wireless access points shall be implemented with Wi-Fi Protected Access 2 with a Pre-Shared Key (WPA2-PSK). This protocol provides the most robust security on the selected wireless access points.5

Another security feature would be implementing firewalls and access control lists (ACLs). These two features can restrict unwanted external traffic. Firewalls work by monitoring suspicious activity by inspecting packets as they pass through routers. Restricting or allowing singular or groups of users can be configured through ACLs, which can often prevent unwanted access to the internal network.

**6.2 Appropriate Security Measures in Liverpool**

Applying the security measures for the Liverpool site will follow the same process as the Manchester site.

**6.3 Addressing External Access and Ensuring Sys-Admin Security**

The need for external access for network administrators to connect to devices remotely will be addressed by implementing Secure Shell (SSH) on each device within the network. SSH protocol ensures the encryption of all data transmissions, including login details, safeguarding the confidentiality of any sensitive company data. Utilising public-key cryptography, the protocol employs mathematical computations to further enhance data protection and confidentiality6.

**7. Conclusion**

Finally, the carefully chosen hardware and software that will be implemented will far outperform the current network infrastructure that is in place now, aligning seamlessly with the company's overall objectives of growth and expansion. Each device underwent thorough consideration during the decision-making process to ensure that the selected technological mix meets the organisation's current needs and strategically positions it for future growth and changing demands. The methodical approach employed in the selection process demonstrates a commitment to obtaining the best available, reliable and effective system, capable of adapting to the changing and dynamic nature of the business's activities. As these carefully chosen devices are integrated, there is a firm expectation that they will contribute synergistically to the company's technological prowess, fostering an environment conducive to innovation, productivity, and seamless adaptation to emerging industry trends.

**8. Bibliography**

**1** Petryschuk, S. (2024) *Classful and classless addressing explained*, *Auvik*. Available at: <https://www.auvik.com/franklyit/blog/classful-classless-addressing/> (Accessed: 7 January 2024).

**2** Cisco (2023) *Understand and use the enhanced interior gateway routing protocol*, *Cisco*. Available at: <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html> (Accessed: 7 January 2024).

**3**(Lorenzen, M. (2021) *The importance of using Vlans to Segment Network Traffic*, *LinkedIn*. Available at: <https://www.linkedin.com/pulse/importance-using-vlans-segment-network-traffic-mike> (Accessed: 14 January 2024).

**3 (image)** Lorenzen, M. (2021) *The importance of using Vlans to Segment Network Traffic*, *LinkedIn*. Available at: <https://www.linkedin.com/pulse/importance-using-vlans-segment-network-traffic-mike> (Accessed: 8 January 2024).

**4** Technologysolutions (2023) *SD Wan features and Benefits*, *Technology Solutions*. Available at: <https://www.technologysolutions.net/blog/sd-wan-features-and-benefits/> (Accessed: 14 January 2024).

**5.** Irei, A. (2022) *Wireless security: WEP, WPA, WPA2 and WPA3 differences*, *Networking*. Available at: <https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2> (Accessed: 8 January 2024).

**6.** Ellingwood, J. (2022) *Understanding the SSH encryption and connection process*, *DigitalOcean*. Available at: <https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process> (Accessed: 12 January 2024).