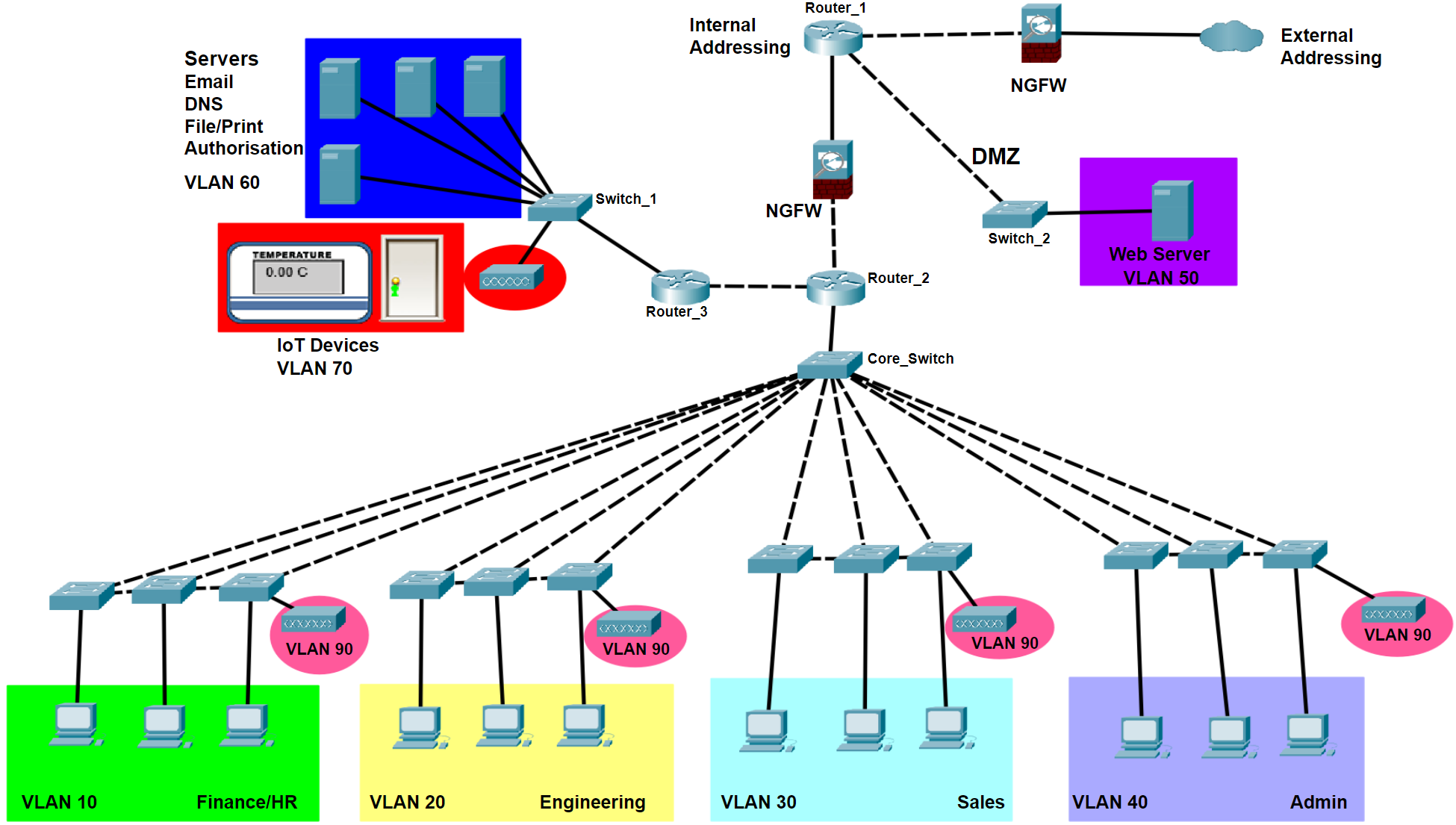
Summative Assessment Report

Word count - 3241

Network Model



1 Introduction

Given the ubiquitous nature of technology, its importance to individuals and businesses is a crucial concern for network architecture. YorkInc’s network has been designed to facilitate: four departments, five servers, wireless devices and Internet of Things (IoT) equipment. Decisions for component choices are justified along with supporting technologies and how the network can be scaled. Security is highlighted with mitigation techniques along with legal and ethical implications for a Bring Your Own Device (BYOB) policy. This report has made the assumption of a single office location.

1.1 Architecture

YorkInc’s network has been designed with the following principles in mind: scalability, availability, security and manageability. Cisco champions these principles into a hierarchical network design as either a three tiered or collapsed core model [[1]](https://www.zotero.org/google-docs/?7IidUm). Importantly, hierarchical design is modular and provides significant advantages over a flat network design. For example: layers have specific functions, there is fault tolerance and changes can be limited to subsections of the network. Overall, management is easier and potential network disruption can be limited [[2]](https://www.zotero.org/google-docs/?zW3dMy). Alternatively, a flat network design would place all connected devices in the same broadcast domain [[3]](https://www.zotero.org/google-docs/?SrbfAR) which would introduce security concerns, slow network throughput and is not scalable.

A collapsed core model has been selected based on YorkInc’s current size. Indeed, Eire, an independent provider of IT services, puts forward that smaller businesses can use a collapsed core to achieve similar benefits to a three tiered model [[4]](https://www.zotero.org/google-docs/?srOeYG). On the other hand, this does come at the cost of fast scalability and the same level of resiliency in a three tiered design. But, given the size of YorkInc and even a hypothetical doubling in network size, the collapsed core model is more than suitable for YorkInc’s current and future requirements. As a point of comparison, a study for a significantly larger business, including twelve buildings each with twenty five floors, selected a three tiered model over a collapsed core due to its size [[5]](https://www.zotero.org/google-docs/?ZJtDgf). This helps illustrate the scale of business required to consider a three tiered model to reap the maximum benefits.

1.2 Firewall and Demilitarised Zone

In order to prioritise security and mitigate malicious actors, a firewall and a Demilitarised Zone (DMZ) have been implemented. Firewalls traditionally work on layers three and four of the Open Systems Interconnection (OSI) model and filter by looking at network traffic based on ports and protocols [[6]](https://www.zotero.org/google-docs/?K47oiM), however can be vulnerable to IP Spoofing. On the other hand, a Next Generation Firewall (NGFW) works on layers two to seven and filters in more sophisticated ways. For instance, by having application level awareness and using deep packet analysis [[7]](https://www.zotero.org/google-docs/?KOiFFT). Adventitiously, there is more scope to identify potential threats when compared to a traditional firewall. Moreover, a NGFW incorporates many newer technologies, such as; an intrusion prevention system, anti-spam, stateful inspection and packet filtering into a Unified Threat Management (UTM) approach. UTM is where one hardware, or software, device provides many security functions [[7]](https://www.zotero.org/google-docs/?THlMhR) which enables a greater level of protection when compared to a traditional firewall. This led to the selection for NGFWs as part of the network design.

A DMZ allows for the web server to be separated from the rest of YorkInc’s internal network to restrict external users' interaction with it. A suitable design choice is to deploy two firewalls, one for the internal network and one for the external network, with the DMZ delineating the space between these two points [[8]](https://www.zotero.org/google-docs/?OM4lF1). Therefore, this security measure has been incorporated into YorkInc’s design.

1.3 IP Address Scheme

When considering the current size and potential growth of the network, IPv4 addressing had to be determined for the Local Area Network (LAN). RFC1918 [[9]](https://www.zotero.org/google-docs/?oXw4Lv) lists the available private IP addresses which can be used on a network, so long as they are not used publicly. This means an internal network is not restricted in choice for the IP address range it uses, so long as the private IP address range is utilised. Lammle highlights that the largest range should be used for enterprise size businesses [[10, p.178]](https://www.zotero.org/google-docs/?b9nep4) to allow for both growth and flexibility. Also considered were the 192.168.0.0 and 172.16.0.0 ranges, however, both have less host spaces and do not scale as well. Indeed, industry best practice documentation from Cisco also supports this view, arguing that if starting a network from scratch then to strongly consider the use of the 10.0.0.0 range [[11]](https://www.zotero.org/google-docs/?KNdfgM). Importantly, the 10.0.0.0 range will allow YorkInc to meet its current addressing requirements and allow for growth. Also, Subnetting can be used to manipulate the internal IP addressing to adapt for any network changes, such as department expansion or new sites. Furthermore, Dynamic Host Configuration Protocol has been incorporated with the Domain Name Service server [[12]](https://www.zotero.org/google-docs/?m23Jqk). This is to provide efficient and fast configuration and also aid network management. While Network Address Translation (NAT) will map internal IP addressing to the public facing IP address [[13]](https://www.zotero.org/google-docs/?vKfm2d).

1.4 Routers

Routers work at layer three of the OSI model and direct packets based on their destination IP addresses [[10]](https://www.zotero.org/google-docs/?k9pgul). Internal routers have been used to segment the network, alongside subnetting, and aid with security while the external router connects YorkInc’s LAN to the internet.

Subnetting is a technique which segments the network at level three of the OSI model and provides benefits, which include; reduced network traffic, optimised network performance, security and scalability [[14]](https://www.zotero.org/google-docs/?GrGsfD). For YorkInc, each department will be assigned a subnet with its own range of usable IP addresses (see *appendix A*). Importantly, subnetting allows for separation of network devices at the IP level which allows for control over department size, with Variable Length Subnet Masks (VLSM), as well as the ability to add new devices or additional departments if required [[15]](https://www.zotero.org/google-docs/?Cl2Ubh). Meaning each department can have its own subnet and communicate with each other, but requires a router to exchange data beyond their subnet. Importantly, network security is increased as subnetting obscures the details of the internal network to routers outside of YorkInc [[16]](https://www.zotero.org/google-docs/?CWjbTZ). This makes it difficult for unauthorised users to gain access to the network and its resources.

1.5 Switches

Switches are a layer 2 component which forward frames to connected network devices, breaking a network up into broadcast domains and making smaller collision domains [[17]](https://www.zotero.org/google-docs/?cV7xpq). Switches provide a significant advantage over hubs, which send all data frames to all connected devices which do not create broadcast domains [[10, p.96]](https://www.zotero.org/google-docs/?88o95F). Thus, switches enable the network to have better performance, more bandwidth and improved security.

Switches also enable VLANs which are used to logically separate a network into smaller broadcast domains by using one switch to act as many [[18]](https://www.zotero.org/google-docs/?gFwMiP). Importantly, this means devices on one VLAN cannot directly communicate with another VLAN without a router, or a layer three switch. This is achieved by a Media Access Control (MAC) learning algorithm which forwards only traffic associated to the VLAN of the port it was received on [[19]](https://www.zotero.org/google-docs/?zc31CD). Advantages for using VLANs are: scalability, security, workgroup creation, cost effectiveness and broadcast control [[3]](https://www.zotero.org/google-docs/?wpzYKx). To illustrate this with the network design, wireless Access Points (AP) have been placed on a VLAN 90 to segregate BYOD network traffic.

Inter VLAN routing is another consideration for the network design. One approach is to use multiple interfaces from individual switches and connect them directly to a router. However, routers may not have enough interfaces and this methodology is not ideal for medium to large networks [[20]](https://www.zotero.org/google-docs/?uTPhKh). A solution is to use ‘router on a stick’ where all department switches are connected to another switch which is in turn connected to a router by a single trunk link using the 802.11q standard [[21, p. 802]](https://www.zotero.org/google-docs/?tgKAoI). Trunking allows for one interface on the router to route the network traffic for multiple VLANs [[22]](https://www.zotero.org/google-docs/?hyRr9l). This means the design of YorkInc’s network can reduce the number of routers through inter VLAN routing by utilising trunking to a single router. Notably, this aids the manageability of the network and can reduce the cost of implementing a component heavy network design.

2 Scalability and Availability

2.1 Layer Three Switch

A layer three switch, also known as a multilayered switch, is a device which can forward frames based on MAC addresses as well as forward packets using an IP destination [[17]](https://www.zotero.org/google-docs/?beCInq). Inclusion of layer three switches in the network will provide benefits for both scalability and availability. For instance, layer three switches are faster than a router on a stick as there is no need for external links to a router in order to provide the routing function and latency is lower due to data not leaving a switch to be routed [[23]](https://www.zotero.org/google-docs/?wToWf5). Replacing the current router on a stick with layer three switches will increase network speeds and reduce the number of physical routers required to route traffic.

2.2 Spanning Tree Protocol

Spanning Tree Protocol (STP) is a supporting technology which is implemented on switches at layer two of the OSI model which allows for redundancy and fault tolerance. This is achieved by providing routes for frames to travel by placing a switch’s ports in a forwarding or blocking state to prevent frame flooding and broadcast storms [[24]](https://www.zotero.org/google-docs/?fNK0zk). Notably, by blocking a port, to another switch, frames are sent in a certain direction but if the current working link goes down the blocked port will go into a forwarding state. It should be noted that advances have been made to improve SPT’s convergence times. For instance, Rapid Spanning Tree Protocol (RSPT) is significantly faster than core STP [[25]](https://www.zotero.org/google-docs/?Z09H62), however hardware delays, such as the detection of a link being down, can increase network convergence times potentially from microseconds into seconds. Ultimately, RSPT improves upon SPT as well as providing availability in the network in case of a link failure.

2.3 Load Balancer

Load balancers allow for incoming traffic to be distributed efficiently to maintain availability of a server and operate on layer four of the OSI model by filtering traffic based on port numbers [[26]](https://www.zotero.org/google-docs/?reMv8g). This allows for servers to not be overwhelmed by a sudden increase in traffic. For example, if there is a high demand in YorkInc’s web server from external traffic, a load balancer will be able to see which server is nearing capacity and divert new traffic to another web server. Notable benefits of including a load balancer are: reduced downtime, redundancy and scalability [[27]](https://www.zotero.org/google-docs/?vtwc0f). Alongside the inclusion of a load balancer the incorporation of additional servers will also be required. Therefore, the future deployment of a load balancer, will assist availability for a larger network as traffic will be distributed evenly.

2.4 Routing Protocols

Open Shortest Path First (OSPF) is a routing protocol which is scalable and uses a link state algorithm. Link state algorithms involve each router keeping three tables, consisting of: neighbour routers, network topology and bandwidth as a metric to calculate the cost of a link [[10, p.385]](https://www.zotero.org/google-docs/?dgILYn). An advantage over distance vector algorithms, such as Routing Information Protocol (RIP), is that link state routers contain a database of links and their status in a network [[28]](https://www.zotero.org/google-docs/?PFsBri). This enables OSPF routers to have accurate and up to date routing information. Importantly, this allows for fast convergence times and adaption to network changes. A further advantage is that OSPF, version 3, allows for subnetting while RIP does not, and support for both IPv4 and IPv6.

An alternative internal routing protocol is Cisco’s proprietary Enhanced Internal Gateway Routing Protocol (EIGRP). EIGRP is an advanced distance vector protocol which also uses aspects of link state protocols as it uses hello packets to discover neighbouring routers and is designed to be scalable [[29]](https://www.zotero.org/google-docs/?7Rg9hF). Moreover, EIGRP checks for changes periodically and updates neighbouring routers with those changes only, in order to minimise bandwidth [27]. However, a disadvantage is that EIGRP only works on Cisco equipment. Arguably, with a small or a large network EIGRP is a good option. Indeed, EIGRP performs better against OSPF using the metrics of convergence and throughput, however OSPF has the least packet delay [[30]](https://www.zotero.org/google-docs/?G8qHjL). Adaptation of EIGRP will also depend on component manufacturer choice balanced with network performance requirements. That being said, a strong argument can be made for the implementation of EIGRP over OSPF given its higher performance metrics.

2.5 Internet Protocol Version 6

IPv4 has underlying issues, the most significant being that IPv4 addresses were depleted in 2011 [[31]](https://www.zotero.org/google-docs/?GOwNza). A work around, proposed in 1993, was the use of NAT so that only a single IP address can be used externally [[32]](https://www.zotero.org/google-docs/?xEyFyv) while private addressing can be used internally [[9]](https://www.zotero.org/google-docs/?sDO8pE). Indeed, Classless Inter-domain Routing, VLSM, and Port Address Translation are also similar technologies for the extension of IPv4. Internet Protocol Version 6 (IPv6), a 128 bit address compared to IPv4’s 32bit, is gradually being implemented to succeed IPv4. With this in mind, it is essential that scalability to IPv6 is considered.

Dual stack enables hosts and routers to communicate simultaneously with IPv4 and IPv6, and tunnelling allows for IPv6 to be transmitted over an IPv4 network using encapsulation [[33]](https://www.zotero.org/google-docs/?85FkD6). Dual stack and tunnelling demonstrate that the requirement for IPv6 adaptation is needed and is gradually being implemented. It should be noted that IPv6 performs better and has fewer overheads when compared against IPv4 [31], [[34]](https://www.zotero.org/google-docs/?8rlpKF). Therefore, YorkInc should strongly consider the long term change from IPv4 to IPv6 and the use of dual stack and tunnelling migration techniques.

3 Security

3.1 Rogue Access Point

Rogue Access Points (RAP) are defined as an unmanaged AP connected to a network without authorisation, with the potential for espionage and launching further attacks [[35]](https://www.zotero.org/google-docs/?Tq8bkT). Significantly, the implications of one being on the network results in integrity and confidentiality being compromised.

In order to mitigate RAPs, physical security of the premises should be considered. Arguably, the most important aspect of a RAP threat is that someone needs to physically connect one into the network. RAPs then provide a backdoor into a network and evade security measures already in place, such as a firewall [[35]](https://www.zotero.org/google-docs/?Qhwrat). Therefore, cabinets containing network components should be locked and staff should have identification to access the premises. Furthermore, unused switch ports can also be disabled to further mitigate a physical ethernet connection [[35]](https://www.zotero.org/google-docs/?XWge3Z) .

Removing the RAP is the next mitigation technique to consider. Samra el al [[36]](https://www.zotero.org/google-docs/?nYD6qA) argues for an approach of filtering RAPs by matching MAC addresses against a list of authorised MAC addresses; dropping APs with MAC addresses not on the list. On the other hand, [[37]](https://www.zotero.org/google-docs/?IUs3Ba) put forward that this RAP detection method has flaws and does not work with every situation. An alternative approach is put forward by Anmulwar el al [[38]](https://www.zotero.org/google-docs/?ZrOxGw) who argue for a hybrid software approach where both client and server side software detection methods are combined. Significantly, a defence in depth approach would allow for multiple mitigation techniques as one is not guaranteed to always catch a RAP.

3.2 Denial of Service

Denial of Service (DoS) attacks are defined as when legitimate network users are unable to access resources on the network [[39]](https://www.zotero.org/google-docs/?ve8u6L). This can be achieved through flooding a network with excessive traffic or blocking access by disrupting connections to communication services at different levels of the OSI model [[26]](https://www.zotero.org/google-docs/?jHxHRC). For instance, jamming attacks occur at the Physical layer, while flood attacks occur at the Data Link layer exploiting weaknesses in MAC address frames. DoS attacks affect the operational capacity of the company, such as the ability to access emails and resources which can cost the company both money and time.

Mitigation for DoS attacks should start with identifying the type of attack followed by isolation of the affected network and blocking the attacking traffic [[40]](https://www.zotero.org/google-docs/?NaDDDN). That being said, Arockiam and Vani [[41]](https://www.zotero.org/google-docs/?XgcKmP) put forward two mitigation algorithms: the Intruder Detector and Manager (IDM), which maintains tables to prevent masquerading DoS attacks, and Letter Envelope Protocol with Traffic pattern filtering (LEPT), which are designed to avoid resource flooding DoS attacks. Notably, these algorithms are effective in tests carried out by the researchers, however, future work on MAC address spoofing is required.

3.3 Man in the Middle

Man in the middle (MITM) attacks are defined as a third party surveying, capturing, altering or sending data between hosts without their knowledge [[42]](https://www.zotero.org/google-docs/?Siddjy). Furthermore, MITM allows for different vectors of attack, including: Address Resolution Protocol (ARP) poisoning, Internet Control Message Protocol redirects and DNS poisoning [[43]](https://www.zotero.org/google-docs/?mtpnN9). With ARP poisoning, the attacker poisons the ARP cache and redirects it to themselves [41] which works on layer 2 of the OSI layer. Consequently, this can lead to the attacker obtaining confidential information, such as passwords or other personal data. Moreover, traffic could be redirected to an external server.

Mitigation for MITM attacks include: static ARP entries for devices in the network, the use of ARP detection tools and the use of VLANs to segment the network [[44]](https://www.zotero.org/google-docs/?ombL14). Arguably, the use of these methods assist in countering a MITM attack, but techniques like static ARP entries require significant overheads [[45]](https://www.zotero.org/google-docs/?dQOVh2). An alternative approach is the use of Wireshark to passively monitor the network [[46]](https://www.zotero.org/google-docs/?TIc6UZ) but it should be noted this will only alert once the attack is taking place.

3.4 Access Point Placement

Placement of APs should be positioned for maximum coverage of an area so users receive strong signal strength. Indeed, walls, doors and windows can reduce signal strength as well as frequencies which can cause interference [[47]](https://www.zotero.org/google-docs/?stOuX5). Therefore, it is important to place the 2.4Ghz range on channels: 1, 6 and 11 to avoid interference. Whereas the 5Ghz range provides 23 non overlapping channels. Optimal placement of APs should be in the centre of a ceiling with different frequency channels assigned to nearby APs to mitigate any interference [[48]](https://www.zotero.org/google-docs/?WUnAWE).

3.5 BYOD

Adoption of a BYOD policy allowing users access to the company’s network comes with potential ethical and legal challenges, such as: security, privacy and storing data [[49]](https://www.zotero.org/google-docs/?TzBgXd). On the other hand, allowing employees to use their own devices is beneficial as owners are familiar with them and the company saves money [[49]](https://www.zotero.org/google-docs/?mGBITd). Moreover, portability allows for flexible working.

Data storage and the company losing the ability to control that data is one issue with BYOD. For example, data leaving an organisation on a device and being stored on an employee’s personal cloud service presents both security implications and potential legal ramifications [[50]](https://www.zotero.org/google-docs/?gtpKOs). Indeed, automatic device back of files could also mean employees are unaware of this issue. Thus, employee training and a clear policy of BYOD use is required to delineate company responsibility for data handling and instruct employees with clear guidelines for use [[51]](https://www.zotero.org/google-docs/?Ui0g4C).

Therefore, a policy to meet the challenges of BYODs should be considered carefully which enables the use of devices for the benefit of employees and with low risk for legal ramifications for the company.

4 Conclusion

In conclusion, this report has considered the network design and underlying protocols with justification for their use. YorkInc’s network is designed for scalability, availability, security and manageability which has been achieved through component choice, use of underlying technologies, mitigation of wireless threats and considering how the network can grow in the future. Three potential wireless network attacks and potential mitigations techniques were considered with a view for multiple layers of defence in depth. Lastly, a BYOD policy is recommended to empower employees while maintaining security and company data.

Reference List

[[1] A. A. Bruno, S. Jordan, and A. A. Bruno, *CCDA 640-864 official cert guide*. Indianapolis, Cisco Press, 2011.](https://www.zotero.org/google-docs/?jZnPm4)

[[2] D. Ran, ‘Design and Planning of University Campus Network’, *J. Phys. Conf. Ser.*, vol. 1533, no. 2, p. 022109, Apr. 2020, doi: 10.1088/1742-6596/1533/2/022109.](https://www.zotero.org/google-docs/?jZnPm4)

[[3] A. C. Odi and N. E. Nwogbaga, ‘The Proposed Roles of VLAN and Inter-VLAN Routing in Effective Distribution of Network Services in Ebonyi State University’, vol. 4, no. 7, 2013.](https://www.zotero.org/google-docs/?jZnPm4)

[[4] E. Systems, ‘What is a Collapsed Core in a Network Design?’, *EIRE Systems*, Nov. 11, 2020. https://www.eiresystems.com/what-is-a-collapsed-core-network/ (accessed Mar. 03, 2023).](https://www.zotero.org/google-docs/?jZnPm4)

[[5] Yanhong Wang, Hanshi Wang, Lizhen Liu, Wei Song, and Jingli Lu, ‘Research and implementation of network planning and design for community’, in *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*, Harbin, China, Dec. 2015, pp. 847–850. doi: 10.1109/ICCSNT.2015.7490873.](https://www.zotero.org/google-docs/?jZnPm4)

[[6] C. Togay, A. Kasif, C. Catal, and B. Tekinerdogan, ‘A Firewall Policy Anomaly Detection Framework for Reliable Network Security’, *IEEE Trans. Reliab.*, vol. 71, no. 1, pp. 339–347, Mar. 2022, doi: 10.1109/TR.2021.3089511.](https://www.zotero.org/google-docs/?jZnPm4)

[[7] J. Liang and Y. Kim, ‘Evolution of Firewalls: Towards Secure Networks Using Next Generation Firewall’, in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, Jan. 2022, pp. 0752–0759. doi: 10.1109/CCWC54503.2022.9720435.](https://www.zotero.org/google-docs/?jZnPm4)

[[8] Associate Professor Department of Computer Science , Dr. Ambedkar Government Arts College, Chennai, India., Dr. K. Shyamala, G. Priyadharshini, and Research Scholar Department Of Computer Science , Dr. Ambedkar Government Arts College, Chennai, India., ‘Rules Assurance: Preventing Unauthorized Access through Building Right Firewall Configuration’, *Int. J. Recent Technol. Eng. IJRTE*, vol. 8, no. 3, pp. 8006–8010, Sep. 2019, doi: 10.35940/ijrte.C6414.098319.](https://www.zotero.org/google-docs/?jZnPm4)

[[9] R. Moskowitz, D. Karrenberg, Y. Rekhter, E. Lear, and G. J. de Groot, ‘Address Allocation for Private Internets’, Internet Engineering Task Force, Request for Comments RFC 1918, Feb. 1996. doi: 10.17487/RFC1918.](https://www.zotero.org/google-docs/?jZnPm4)

[[10] T. Lammle, *CCNA routing and switching complete study guide*, Second edition. United States, Sybex, a Wiley brand, 2016.](https://www.zotero.org/google-docs/?jZnPm4)

[[11] ‘IP Addressing Guide’, *Cisco*. https://www.cisco.com/c/dam/global/en\_ca/solutions/strategy/docs/sbaBN\_IPv4addrG.pdf (accessed Mar. 03, 2023).](https://www.zotero.org/google-docs/?jZnPm4)

[[12] A. Yasin, M. Elfarizi, M. N. A. Nirky, M. Ravil, and Z. A. Safitri, ‘A DESIGN OF DHCP SERVER, WEB SERVER AND DNS SERVER USING CISCO PACKET TRACER’, *JComce - J. Comput. Sci.*, vol. 1, no. 1, Art. no. 1, Jan. 2023, Accessed: Mar. 01, 2023. [Online]. Available: https://jurnal.teknologiriau.net/index.php/jcomce/article/view/47](https://www.zotero.org/google-docs/?jZnPm4)

[[13] M. Smith and R. Hunt, ‘Network security using NAT and NAPT’, in *Proceedings 10th IEEE International Conference on Networks (ICON 2002). Towards Network Superiority (Cat. No.02EX588)*, Singapore, 2002, pp. 355–360. doi: 10.1109/ICON.2002.1033337.](https://www.zotero.org/google-docs/?jZnPm4)

[[14] S. Sisat, ‘IP Subnetting’, *Int. J. Knowl. Eng. Soft Data Paradigm.*, vol. 2, pp. 5–10, Mar. 2013.](https://www.zotero.org/google-docs/?jZnPm4)

[[15] A. Manaf and D. S. Bataona, ‘Analysis and design of subnetting methods: Hybrid fixed length subnet masking (HFLSM)’, in *2014 International Conference on Electrical Engineering and Computer Science (ICEECS)*, Kuta, Bali, Indonesia, Nov. 2014, pp. 102–108. doi: 10.1109/ICEECS.2014.7045228.](https://www.zotero.org/google-docs/?jZnPm4)

[[16] W. R. Stevens, ‘TCP/IP Illustrated’.](https://www.zotero.org/google-docs/?jZnPm4)

[[17] W. Stallings, *Data and computer communications*, 8th ed. Upper Saddle River, N.J: Pearson/Prentice Hall, 2007.](https://www.zotero.org/google-docs/?jZnPm4)

[[18] A. I. Mathew, ‘A STUDY ON VIRTUAL LOCAL AREA NETWORK (VLAN) AND INTER-VLAN ROUTING’, vol. 4, no. 10, 2017.](https://www.zotero.org/google-docs/?jZnPm4)

[[19] O. Bonaventure, ‘Computer Networking : Principles, Protocols and Practice’.](https://www.zotero.org/google-docs/?jZnPm4)

[[20] ‘Inter-VLAN Routing > Objectives | Cisco Press’. https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=4. (accessed Mar. 02, 2023).](https://www.zotero.org/google-docs/?jZnPm4)

[[21] ‘IEEE 802.1: 802.1Q-2014 - Bridges and Bridged Networks’. https://www.ieee802.org/1/pages/802.1Q-2014.html (accessed Mar. 03, 2023).](https://www.zotero.org/google-docs/?jZnPm4)

[[22] I. Ahmad, Dr. J. Ashraf, and Dr. A. R. Nasir, ‘Design and Implementation of Network Security using Inter-VLAN-Routing and DHCP’, *Asian J. Appl. Sci. Technol.*, vol. 04, no. 03, pp. 37–44, 2020, doi: 10.38177/ajast.2020.4306.](https://www.zotero.org/google-docs/?jZnPm4)

[[23] ‘Inter-VLAN Routing. Inter-VLAN Routing | Cisco Press’. https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=4 (accessed Mar. 03, 2023).](https://www.zotero.org/google-docs/?jZnPm4)

[[24] F. Shahriar and J. Fan, ‘Performance Analysis of FHRP in a VLAN Network with STP’, in *2020 IEEE 3rd International Conference on Electronics Technology (ICET)*, Chengdu, China, May 2020, pp. 814–818. doi: 10.1109/ICET49382.2020.9119624.](https://www.zotero.org/google-docs/?jZnPm4)

[[25] R. Pallos, J. Farkas, I. Moldovan, and C. Lukovszki, ‘Performance of rapid spanning tree protocol in access and metro networks’, in *2007 Second International Conference on Access Networks & Workshops*, Ottawa, ON, Canada, 2007, pp. 1–8. doi: 10.1109/ACCESSNETS.2007.4447112.](https://www.zotero.org/google-docs/?jZnPm4)

[[26] J. F. Kurose and K. W. Ross, *Computer networking: a top-down approach*, 6th ed. Boston: Pearson, 2013.](https://www.zotero.org/google-docs/?jZnPm4)

[[27] P. Kumar and R. Kumar, ‘Issues and Challenges of Load Balancing Techniques in Cloud Computing: A Survey’, *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–35, Nov. 2019, doi: 10.1145/3281010.](https://www.zotero.org/google-docs/?jZnPm4)

[[28] I. J. Okonkwo and I. Douglas, ‘Comparative Study of EIGRP and OSPF Protocols based on Network Convergence’, *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, 2020, doi: 10.14569/IJACSA.2020.0110605.](https://www.zotero.org/google-docs/?jZnPm4)

[[29] ‘Understand and Use the Enhanced Interior Gateway Routing Protocol’, *Cisco*. https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html (accessed Mar. 03, 2023).](https://www.zotero.org/google-docs/?jZnPm4)

[[30] A. Manzoor, M. Hussain, and S. Mehrban, ‘Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols’, *Comput. Stand. Interfaces*, vol. 68, p. 103391, Feb. 2020, doi: 10.1016/j.csi.2019.103391.](https://www.zotero.org/google-docs/?jZnPm4)

[[31] ‘Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied - ICANN’. https://www.icann.org/resources/press-material/release-2011-02-03-en (accessed Mar. 01, 2023).](https://www.zotero.org/google-docs/?jZnPm4)

[[32] P. F. Tsuchiya and T. Eng, ‘Extending the IP internet through address reuse’, *ACM SIGCOMM Comput. Commun. Rev.*, vol. 23, no. 1, pp. 16–33, Jan. 1993, doi: 10.1145/173942.173944.](https://www.zotero.org/google-docs/?jZnPm4)

[[33] S. Aravind and G. Padmavathi, ‘Migration to Ipv6 from IPV4 by dual stack and tunnelling techniques’, in *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, Avadi,Chennai, India, May 2015, pp. 107–111. doi: 10.1109/ICSTM.2015.7225398.](https://www.zotero.org/google-docs/?jZnPm4)

[[34] M. R. A. Ahmed and S. S. A. Shaikhedris, ‘Network Migration and Performance Analysis of IPv4 and IPv6’, in *2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, Khartoum, Sudan, Feb. 2021, pp. 1–6. doi: 10.1109/ICCCEEE49695.2021.9429664.](https://www.zotero.org/google-docs/?jZnPm4)

[[35] L. Ma, A. Y. Teymorian, X. Cheng, and M. Song, ‘RAP: protecting commodity wi-fi networks from rogue access points’, in *The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness & Workshops*, Vancouver Canada, Aug. 2007, pp. 1–7. doi: 10.1145/1577222.1577252.](https://www.zotero.org/google-docs/?jZnPm4)

[[36] C. Yang, Y. Song, and G. Gu, ‘Journal of Scientific and Technical Advancements’, vol. 1, no. 3.](https://www.zotero.org/google-docs/?jZnPm4)

[[37] B. Alotaibi and K. Elleithy, ‘Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions’, *Wirel. Pers. Commun.*, vol. 90, no. 3, pp. 1261–1290, Oct. 2016, doi: 10.1007/s11277-016-3390-x.](https://www.zotero.org/google-docs/?jZnPm4)

[[38] S. Anmulwar, S. Srivastava, S. P. Mahajan, A. K. Gupta, and V. Kumar, ‘Rogue access point detection methods: A review’, in *International Conference on Information Communication and Embedded Systems (ICICES2014)*, Chennai, India, Feb. 2014, pp. 1–6. doi: 10.1109/ICICES.2014.7034106.](https://www.zotero.org/google-docs/?jZnPm4)

[[39] C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, *Security in computing*, Fifth edition. Upper Saddle River, NJ: Prentice Hall, 2015.](https://www.zotero.org/google-docs/?jZnPm4)

[[40] D. R. Raymond and S. F. Midkiff, ‘Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses’, *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, Jan. 2008, doi: 10.1109/MPRV.2008.6.](https://www.zotero.org/google-docs/?jZnPm4)

[[41] L. Arockiam and B. Vani, ‘Security algorithms to prevent Denial of Service (DoS) attacks in WLAN’, 2012.](https://www.zotero.org/google-docs/?jZnPm4)

[[42] M. Conti, N. Dragoni, and V. Lesyk, ‘A Survey of Man In The Middle Attacks’, *IEEE Commun. Surv. Tutor.*, vol. 18, no. 3, pp. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.](https://www.zotero.org/google-docs/?jZnPm4)

[[43] G. Nath Nayak and S. Ghosh Samaddar, ‘Different flavours of Man-In-The-Middle attack, consequences and feasible solutions’, in *2010 3rd International Conference on Computer Science and Information Technology*, Chengdu, China, Jul. 2010, pp. 491–495. doi: 10.1109/ICCSIT.2010.5563900.](https://www.zotero.org/google-docs/?jZnPm4)

[[44] B. Pingle, A. Mairaj, and A. Y. Javaid, ‘Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use’, in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, Rochester, MI, May 2018, pp. 0192–0197. doi: 10.1109/EIT.2018.8500082.](https://www.zotero.org/google-docs/?jZnPm4)

[[45] D. Bruschi, A. Ornaghi, and E. Rosti, ‘S-ARP: a secure address resolution protocol’, in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, Las Vegas, Nevada, USA, 2003, pp. 66–74. doi: 10.1109/CSAC.2003.1254311.](https://www.zotero.org/google-docs/?jZnPm4)

[[46] H. Iqbal and S. Naaz, ‘Wireshark as a Tool for Detection of Various LAN Attacks’, *Int. J. Comput. Sci. Eng.*, vol. 7, no. 5, pp. 833–837, May 2019, doi: 10.26438/ijcse/v7i5.833837.](https://www.zotero.org/google-docs/?jZnPm4)

[[47] A. Mc Gibney, M. Klepal, and D. Pesch, ‘A wireless local area network modelling tool for scalable indoor access point placement optimization’, in *Proceedings of the 2010 Spring Simulation Multiconference*, Orlando Florida, Apr. 2010, pp. 1–8. doi: 10.1145/1878537.1878707.](https://www.zotero.org/google-docs/?jZnPm4)

[[48] G. R. Gopal and B. D. Rao, ‘Throughput and Delay Driven Access Point Placement’, in *2019 53rd Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, Nov. 2019, pp. 1010–1014. doi: 10.1109/IEEECONF44664.2019.9048803.](https://www.zotero.org/google-docs/?jZnPm4)

[[49] M. Dhingra, ‘Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)’, *Procedia Comput. Sci.*, vol. 78, pp. 179–184, 2016, doi: 10.1016/j.procs.2016.02.030.](https://www.zotero.org/google-docs/?jZnPm4)

[[50] K. Downer and M. Bhattacharya, ‘BYOD Security: A New Business Challenge’, in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, Chengdu, China, Dec. 2015, pp. 1128–1133. doi: 10.1109/SmartCity.2015.221.](https://www.zotero.org/google-docs/?jZnPm4)

[[51] B. Alotaibi and H. Almagwashi, ‘A Review of BYOD Security Challenges, Solutions and Policy Best Practices’, in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Apr. 2018, pp. 1–6. doi: 10.1109/CAIS.2018.8441967.](https://www.zotero.org/google-docs/?jZnPm4)

Appendix A - IP and Subnet Addressing

