COMP2250 Proposal

Introduction

When designing a network, the objective should not be to achieve the highest quality possible. A business should first understand their intended use for the network, their business requirements, and the network constraints. With this information, a network can be designed to ensure that these needs are met whilst keeping costs to a minimum. With this methodology, an appropriate network will be designed for Bancroft Systems, with the goal of value and maximum return on investment.

Bancroft Systems' Wireless Network (Warehouse)

Many external factors need to be considered when designing and configuring a wireless networking solution. Business requirements, technical requirements, and any constraints caused by the network's expected physical environmental must first be investigated. From this information, the wireless solution can be designed within the bounds of the constraints whilst meeting all the identified requirements as accurately as possible.

Bancroft Systems' Business Requirements

Through use of this methodology, Bancroft Systems have clearly stated the following business requirements. Strong wireless coverage is required throughout the entire area of the warehouse so that workers can use scanning equipment from any position to update an existing warehouse stock database, a crucial aspect of the warehouse. The use of the network will be limited and will only be utilised by a few workers at a time. Finally, there is a low bandwidth requirement, and the tasks that will be performed using the network are not bandwidth intensive.

Warehouse Network Constraints

Now that the requirements have been clearly identified, constraints must also be investigated to understand the bounds of the potential solution. Bancroft Systems have only stated the size of the warehouse, which is 100 meters in length, 40 meters in width and 15 meters in height. However, it would also be valuable to understand the material of the walls and roof, any existing electromagnetic interference within the area, and the number, size, and material of the physical obstacles and objects used within the warehouse area. Given that these critical details have not been provided, multiple solutions should be conceived so that a best fit solution can be chosen based on each solution's advantages and disadvantages.

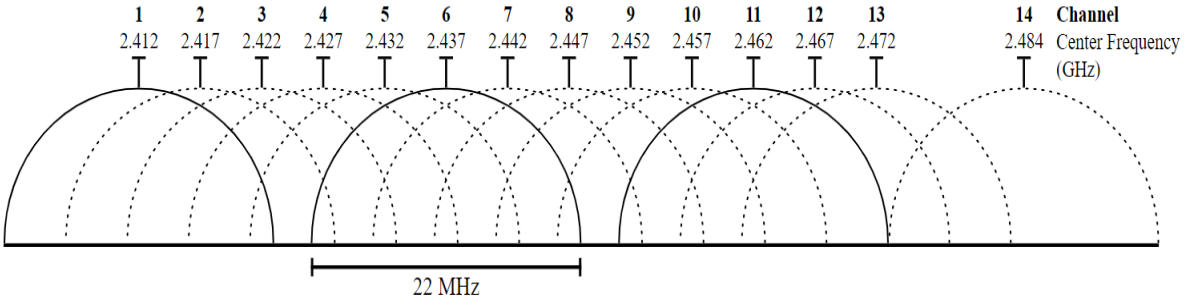
802.11x Technology

There are many different variants of wireless networking technologies. 802.11 refers to the family of wireless LAN (WLAN) standards developed by the IEEE [1]. The sequence of characters that follow, such as "n", "ac", "ax", etc, refers to the generation within that family. WLAN hardware, such as an access point (AP), will implement at least one of these 802.11 generations [1]. It can also be assumed that each subsequent generation of 802.11x will be more expensive than its predecessor. For example, an access point (AP) using the 802.11ac standard will often be more expensive than an AP using the 802.11n standard. Using these standards, we can benchmark the expected performance of different hardware to make more informed decisions.

The most common method of wireless communication makes use of the electromagnetic spectrum, commonly referred to as radio waves [2]. Data is encoded and used to manipulate the waves which are transmitted over-the-air [2]. A key aspect of this technology is the use of frequency bands to allow for more efficient use of the electromagnetic spectrum [3]. This means that electromagnetic spectrum has been divided up and its use has been categorised. For example, in Australia, the 2.4GHz radio frequency range for "Low Interference Potential Devices" is between 2400 and 2483.5 MHz [4], commonly used with WLAN devices. Sending and receiving devices will operate within this frequency range and will ignore waves of other frequencies.

The two most common frequency bands used for WLAN are the 2.4 GHz and 5 GHz range [1]. These different values represent their wave frequency in the electromagnetic spectrum. An electromagnetic wave has different physics properties depending on its length. A longer wavelength will travel further and penetrate solid objects more effectively and shorter wavelengths do not penetrate solid objects as well and do not travel as far [5]. However, the 5 GHz frequency band has a much higher total frequency width [6], allowing for either larger sized channels, massively increasing bandwidth, or reducing interference. Given these details, a 2.4GHz WLAN solution is a more suitable choice for Bancroft Systems due to the size of the warehouse, low bandwidth requirement, and the potential for many physical obstacles.

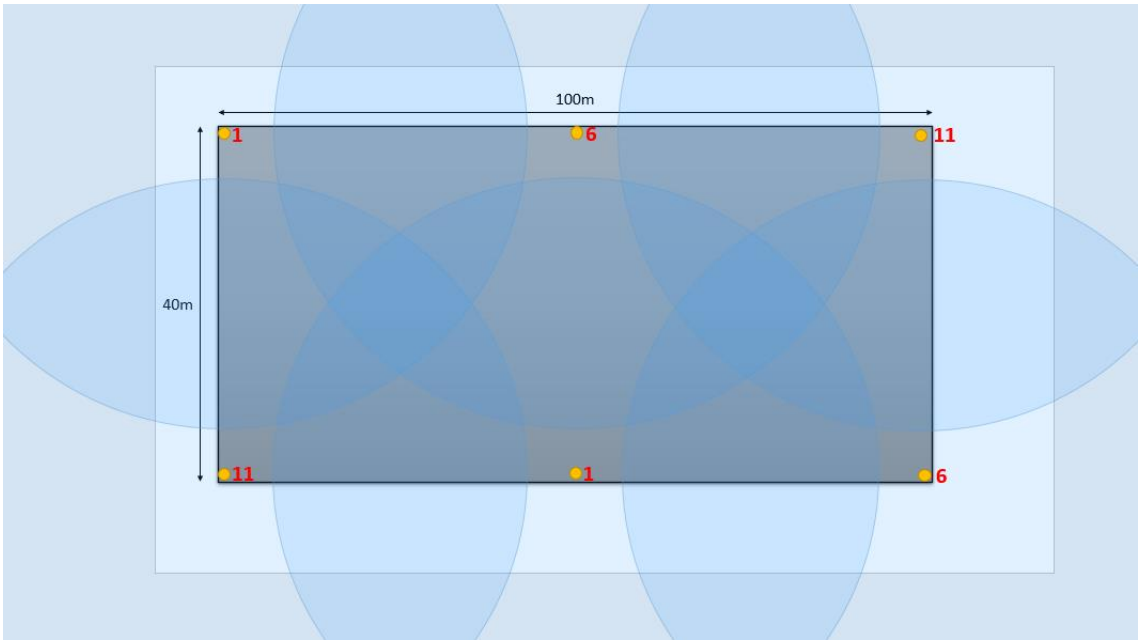
WLAN technologies implement similar techniques, allowing for multiple channels across the frequency bands they operate in. The 2.4 GHz band is dissected into a total of 14 channels to allow for efficient use of the allowable radio frequency range [7]. These values are determined by the country of which the network is in, as each nation has set their own radio frequency regulations. For example, the 2.4GHz frequency band consists of a total width of 83.5MHz in Australia, further broken down into 13 channels of 20 MHz width [4]. Given that 13 channels with a width of 20 MHz equals a total of 160 MHz, channels must overlap one another to fit within the 83.5 MHz requirement.



Radio waves are a half-duplex networking medium, meaning that data can only flow in a single direction cannot be both sent and received at the same time [8]. To alleviate the issues of lost data, like the Ethernet protocol, 802.11x implements Carrier-Sense Multiple Access (CSMA) and Collision Avoidance (CA) to manage the network when collisions do occur [9]. This is important to understand as CSMA/CA protocols consume most of the bandwidth. In a best-case scenario, and whilst controlling all possible variables, real world bandwidth speeds can only reach 50% of the theoretical maximum [10]. These inefficiencies cause by CSMA/CA protocols only become worse as the number of users increase [10].

Access Point Placement

When designing a WLAN solution, overlapping channels are undesirable and increases the probability of wave collision. Within the usable channels 13 usable channels of 2.4 GHz, channels 1, 6 and 11 with a width of 20 MHz do not overlap [6]. This reducing wave collision risks and improving the efficiency of the network. When positioning the wireless access points (WAPs) around the warehouse to achieve strong and complete coverage, these channels can be used to minimise collisions between each other. With a typical AP using the 802.11n standard, a range of 50 meters can be expected indoors [11]. This range value can be impacted by the size, number, and material of the physical obstacles. Below is a concept diagram of WAP placements around the warehouse, including each WAP's frequency channel to best manage wave collision and maximise the wireless network's efficiency. The yellow circles represent the position of an access point, the light blue circles and blue area represent estimated coverage with an assumed 40-meter range, and the red numbers represent the channel of the access point.



Chosen Solution

Through careful consideration of Bancroft Systems' business requirements and our understanding of the physical constraints of the warehouse, the most appropriate solution would be the use of six wireless access points strategically positions around the warehouse. This will ensure that the Bancroft Systems' warehouse staff have strong signal at all locations of the warehouse. Each of these access points should implement the 802.11n standard as this best meet the business requirements whilst keeping costs to a minimum, maximising Bancroft Systems' return on investment. These access points should be positioned in such a way that it matches the previous diagram of this report, which have been carefully placed to maximise wireless coverage of the warehouse. The access points should be configured to use the 2.4 GHz frequency band as this will maximise their reach and allow them to penetrate any unplanned physical obstacles as best as possible, minimising wireless blackspots and inefficiencies for the staff. Each of the access points should be configured to match the appropriate frequency channels as per the above diagram. Each access point should be configured with a channel width of 20 MHz to minimise wave collisions and maximise wireless efficiency, improving all aspects of the business. This design and configuration will best meet the Bancroft System's business requirements whilst appropriately managing the constraints caused by the physical layout of the warehouse.

Bancroft Systems' Network Security Posture

The security of a network can be very complicated, must consider many known and unknown variables, and is best managed with an effective cybersecurity strategy. Cyber risk has been escalated through the rise of cybercrime, the large-scale negative publicity it causes for businesses, and the rapidly growing number of cyberattacking methods. Adequate management of a company's cyber landscape is crucial. However, given the massive number of variables, no one size fits all cybersecurity solution exists. Furthermore, a company's cyber objective should be to maximise return on investment for every dollar spent on cyber protection. This does not necessary look like an expensive and near impenetrable cyber front but should also include a strategy around expense mitigation and recouperation if, and when, a cyber-attack occurs. With a strategy focused on return on investment, a company can rest easy knowing they have planned for breach, and contingency plans are used to manage the event's overall business expense.

Return On Investment Cyber Security Strategy

Bancroft Systems should not seek to patch every hole of their existing cyber landscape. Whilst attempting to block all entrances and stop all attacks is the most desirable outcome, it is not realistic. Cyber criminals only need to find one vulnerability in the network, whereas businesses must attempt to manage all possible

vulnerabilities. Cyber strategies based around preventing all cyber-attack possibilities are not only near impossible, but incredibly expensive. It is proposed that Bancroft Systems adopt a strategy based around return on investment. At its core, this involves adequately balancing monetary and resource investments into cyber security solutions and processes, cyber forensics tooling, and cyber insurance. This strategy inherently understands the risks of the cyber landscape, comprehends the uphill battle for the company, and plans for the breach. A business should invest in core cyber security products with high value propositions and return on investment per dollar spent. These appliances, applications and processes should aid in the prevention of most cyber threats. Investments into an appropriate level of cyber insurance should be adopted. The level of cover should be chosen based on Bancroft Systems' business requirements, cyber risk analysis, and the estimated expenses that occur should a cyberattack occur. Finally, investments of effective cyber forensics tooling are used to prove Bancroft Systems' case to the insurance company when a cyber-attack occurs. Investments into these three aspects of the strategy will ensure a maximum return on investment regarding Bancroft Systems' cyber spending.

Crucial Cyber Security Appliances, Applications, and Processes

Using the proposed return on investment cyber security strategy, Bancroft Systems should consider the following core cyber security appliances, applications, and processes. Implementing the following suggestions will ensure that Bancroft Systems have a strong cyber landscape, protecting the company from most threats, whilst maintaining a focus on value for money.

Firewall

The first crucial appliance that should be implemented is an enterprise grade next-generation firewall. Firewalls sit in front of an entire network and all traffic must pass through a firewall before reaching the external facing network router. The firewall's purpose is the either allow or block external network traffic using a set of rules. Rules can be set to not only prevent cyber threats, but also to prevent outbound traffic from employees or internal stakeholders alike from accessing undesirable network traffic. Firewalls provide stateful inspection of network traffic, bringing smarts to the firewall and allowing it to make informed decisions and threat analysis based on the network packet. Next-generation firewalls take this concept to the next level, implementing application-level inspection, awareness, and control. Furthermore, next-generation firewalls often include integrated intrusion detection and prevention processes, maximising cyber protection and value for money from a single appliance. A firewall is a company's first line of defence and is a crucial aspect of network security the Bancroft Systems should implement [12].

Endpoint Protection

Another crucial application that should be implemented into the Bancroft Systems' repertoire is endpoint protection. This application will be installed onto and monitor the end-user devices of a network such as personal computers, laptops, smartphones, printers, cameras, etc. The purpose pf endpoint security is to detect intrusion, malware, ransomware, or any other form of cyber-attack and prevent it from creating further issues within a network. In contrast to a firewall, endpoint security applications act as a last line of defence, stopping cyber threats that may have made it through a firewall or any other cyber security appliance. The endpoint security industry have made many recent and crucial innovations causing traditional anti-virus to become relatively obsolete. When choosing an appropriate endpoint security solution, Bancroft Solutions should consider the following features. Firstly, Bancroft Systems should choose a technology built around machine learning. These applications outperform traditional signature based anti-virus [13] due to its ability to identify new threats quickly and prevent them causing damage. Often, machine learning based endpoint security applications operate as a mesh-like network with use of the cloud, meaning that all endpoints using the software globally will learn from each other endpoint, maximising cyber protection and return on investment. Secondly, Bancroft Systems should select an endpoint security solution that includes an in-built management platform, allowing for easier management of cyber threats. This will provide a clearer analysis of the existing cyber threat landscape and allow management to make informed decisions to improve upon the Bancroft Systems' cyber strategy. Endpoint protection is crucial, acts as a last line of defence, and will protect Bancroft Systems from many cyber threats and should be implemented.

Disaster Recovery

In the modern world of business, appropriate data collection, use and analysis is crucial for when streamlining, automating, and creating business process efficiencies. In the event of a cyber-attack, or an event that causes a failure of the database, this data can be inaccessible, lost, corrupted, or destroyed. This can leave the business in a vulnerable state, drastically reducing process efficiency, or, worst-case, stops a business from functioning at all. Disaster recovery is a process implemented by many businesses globally of which data is stored and secured in multiple physical locations. In the event of an emergency, and when data is lost, the disaster recovery site will be utilised allowing for the business to continue its operations as normal as possible. The implementation of a disaster recovery site will massively increase Bancroft Systems' level of redundancy, allowing them to continue business operations in the event of a cyber-attack or any other form of emergency that causes data loss.

Employee Cyber Security Awareness Training

Nearly all companies implement cyber security appliances, applications and processes of some kind. Many of these tools are used to monitor, identify, and prevent a multitude of cyber related threats. These tools are incredibly effective at preventing many different forms of brute force attacks. However, these tools are also used to manage the threat of human error caused by the internal employees and stakeholders of the company. According to Cybint, 95% of all cybersecurity breaches are caused by human error [14]. Phishing is a type of social engineering attack often used by cyber criminals targeting internal stakeholders [15]. This method seeks to gain access to a network by portraying a friendly character, often trying to convince unsuspecting people to click on a link, open or download a file, or install software, all with the malicious intent. IBM's 2021 study found that 33% of cyber-attacks were caused by some form of phishing [16]. These statistics display that, no matter the level of investment into cybersecurity, people are often the weakest link of a network. Hence, adequate cybersecurity and awareness training should be provided to all stakeholders that have any level of access to the network. Whilst this does not guarantee results, training will reduce risks of these stakeholders being caught out by phishing or similar cyberattacks. This training will also assist when making cyber insurance claims, will act as proof that Bancroft Systems has attempted to mitigate all reasonable risks human error risks, and improve the speed of which an insurance company will pay Bancroft Systems to alleviate damages occurred from cyberattacks. Cyber security and awareness training is a crucial aspect of cyber threat mitigation and should be implemented by Bancroft Systems to maximise their cyber security posture.

Cyber Insurance

The core principles of this cyber strategy revolve around the concept that cyberattacks are inevitable. Cyber insurance is one of the most important aspects of this strategy and is used to mitigate the financial expenses caused by cyberattacks. Depending on chosen cover, cyber insurance can cover expenses such as loss of revenue due to business interruptions, hiring negotiators and paying ransoms, defence against legal claims, marketing expenses, etc. Bancroft Systems should first perform a risk analysis of their existing cyber security landscape. Once this information has been uncovered, it can be used to select an appropriate level of insurance cover to suit these risks and estimated expenses that could occur. With an appropriate cyber insurance policy, Bancroft Systems can have a higher level of confidence that risk of failed business operations and unexpected costs of any type will be mitigated. This will allow the business to focus on providing value to their customer base and scale without fear of their growing cyber footprint and the inherent risks this creates.

Cyber Forensics Tools

As Bancroft Systems scale their network, the risk of cyber threats increases. With the adoption of a strong and well thought out cyber insurance policy to mitigate financial and any other resource expenses of an attack, rapid and solid insurance claims are a must. This means when Bancroft Systems seek to make a claim against their chosen cyber insurance policy, strong and complete evidence of the attack, the cause, and the damages must be quickly collected and provided to the insurance company. Given that an insurance company business model inherently seeks to either delay payment, only provide partial payment, or not fulfill the claim's payment request at all, evidence of a cyberattack claim will allow Bancroft Systems to maximise the effectiveness and speed of any cyber insurance claims. This will ensure that Bancroft Systems maintain a high

level of operational uptime, minimal expense, and quick alleviation of any damages caused. Cyber forensics tools used to collect accurate evidence and quickly build strong insurance claim cases should be implemented by Bancroft Systems to maximise their return on investment of their cyber security strategy.

Bancroft Systems' WAN Solutions

As Bancroft Systems expands as a business, adequate management of a networked sprawled over many locations is critical efficient networking communications, network management, and network security. Wide Area Networks (WANs) are used to connect multiple sites or locations together allowing, not only communication between the sites, but more effective management and monitoring of a network as it grows with the business. Given that Bancroft Systems has now grown from one single office to two sites in total, the business must now consider its strategy around how it will enable cross-site networking. As Bancroft Systems have not provided clear requirements of a WAN solution, the following assumptions will be made based on previous specifications, business requirements, and networking constraints. A total of two different WAN solutions will be proposed, each with their own advantages and disadvantages, of which Bancroft Systems will be able to choose the more appropriate proposition. The assumptions include minimal cost, strong level of network management, scalable WAN solution, and can utilise multiple different methods of data transmission.

WAN's Evolving Business Requirements

Traditionally, WAN solutions involved the use of expensive MPLS cabling purchased from a telecommunications provider to privately connect a company's many sites together. Often, this technology would be used to connect all remote sites to the company's head office or main data centre. A complex routing and load-balancing system would be the centre point of all company network traffic. This system would route the traffic to its intended destination, whether it be to an on-premises server hosting critical business applications, or to the broader internet to load a standard website. This not only connected the many locations of a company enabling communication, but it also enabled the performance of network security duties.

As the consumption of business applications have begun moving from on-premises to cloud or Software as a Service (SaaS) consumption models, the requirements for the flow of data has drastically changed. An excellent example of this transition is the birth of Salesforce.com, who provide a popular customer relationship management (CRM) application through the browser. This is consumed using a SaaS business model and has, for the most part, removed any upfront CAPEX expenses in favour of a predictable pay-for-use OPEX model. Whilst this alone is a desirable outcome, the CRM platform also removed update and management requirements and the platform is highly accessible, efficient, and reliable.

Furthermore, networking innovations including high-speed broadband and the use of the 4G/LTE mobile network began to outperform traditional MPLS cabling WAN solutions with massively decreased costs. Traditional router centric WAN models struggled to implement these communication advancements and concept of sending all traffic to a company's head office became expensive and slow in comparison. On top of all of this, Covid-19 initiated the 'Great Resign', the name for the recent growing trend of employees opting for employment opportunities that provide improved work-life balance [17].

Clearly summarised, these key influences have caused several new business challenges. Companies having begun choosing cloud and SaaS consumption models. With the introduction of newer networking technologies, traditional MPLS connections have a weaker value proposition, providing slower less reliable solutions at higher costs. And finally, companies must begin adapting to the evolving employee landscape and their expectations of increase work-life balance, meaning that networking solutions must be able to manage networking and security of traffic originating from any location, on any device, at any time.

SD WAN

Given these challenges, the software defined wide area network (SD WAN) seeks to solve most of these issues, enabling the management of all traffic, across any networking medium, dependant on the applications requirement. As companies began moving towards cloud and SaaS based business application, the routing internet destined traffic through a company's data centre is not only slower and less efficient, but it also

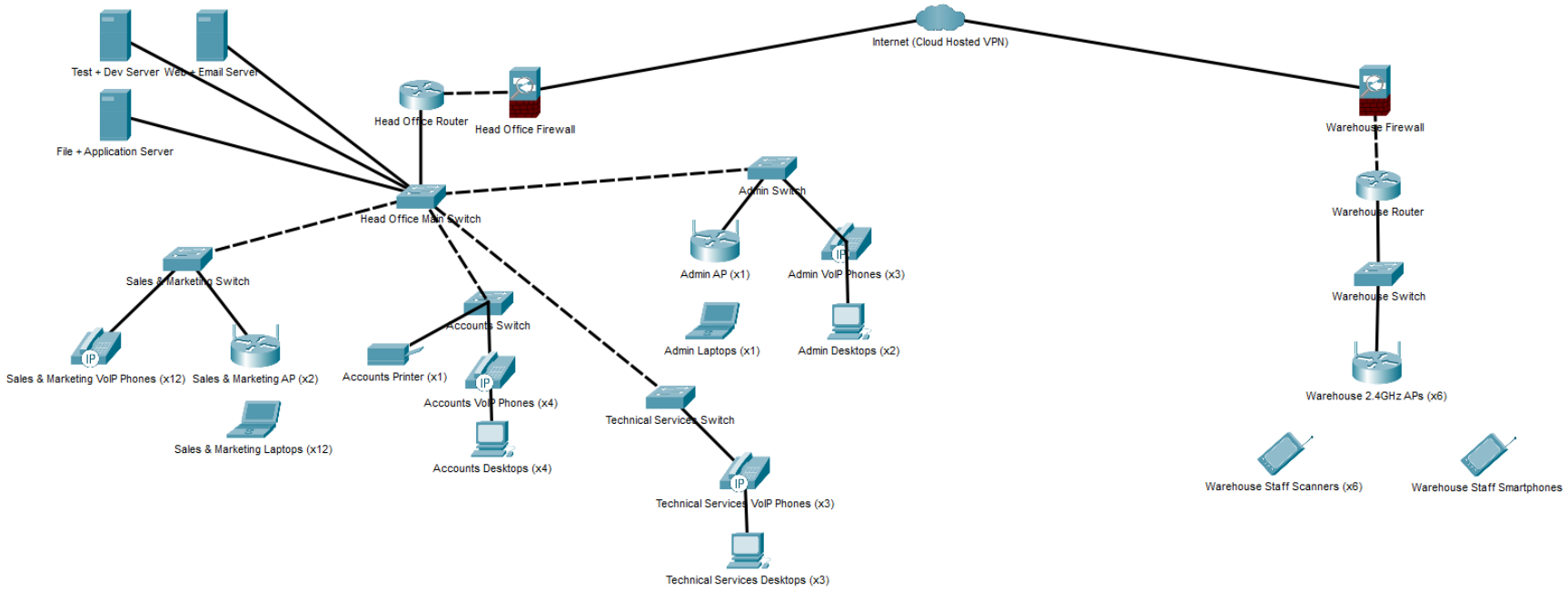
wastes expensive networking and computation resources. SD WAN allows for the automation, orchestration, redundancy, and simple management of how network traffic should be routed on an application basis. For example, if an employee is working from home and attempts to access Salesforce.com, the traffic does not need to be routed through the data centre but can use the employees home broadband connection. This drastically increases networking efficiency, the traffic speed for the end-user, and removes the waste of company networking resources. As an SD WAN solution is primarily built around a software defined solution, routing, priority, and any other means of rules can be created, allowing for maximum customisation of the network and its use. An SD WAN solution paired with a dedicated MPLS connection between the head office and the warehouse would allow for simple, scalable, secure, and an easy to manage network. However, whilst an SD WAN solution solves nearly all networking challenges for a business of any size, this solution is expensive and would predominantly be funded through an upfront CAPEX cost. Hence, this powerful solution is most likely overkill for a company with only 33 employees. Often, SD WAN solves these challenges for large enterprises that manage hundred, if not thousands, of employees using many business-critical applications.

VPN

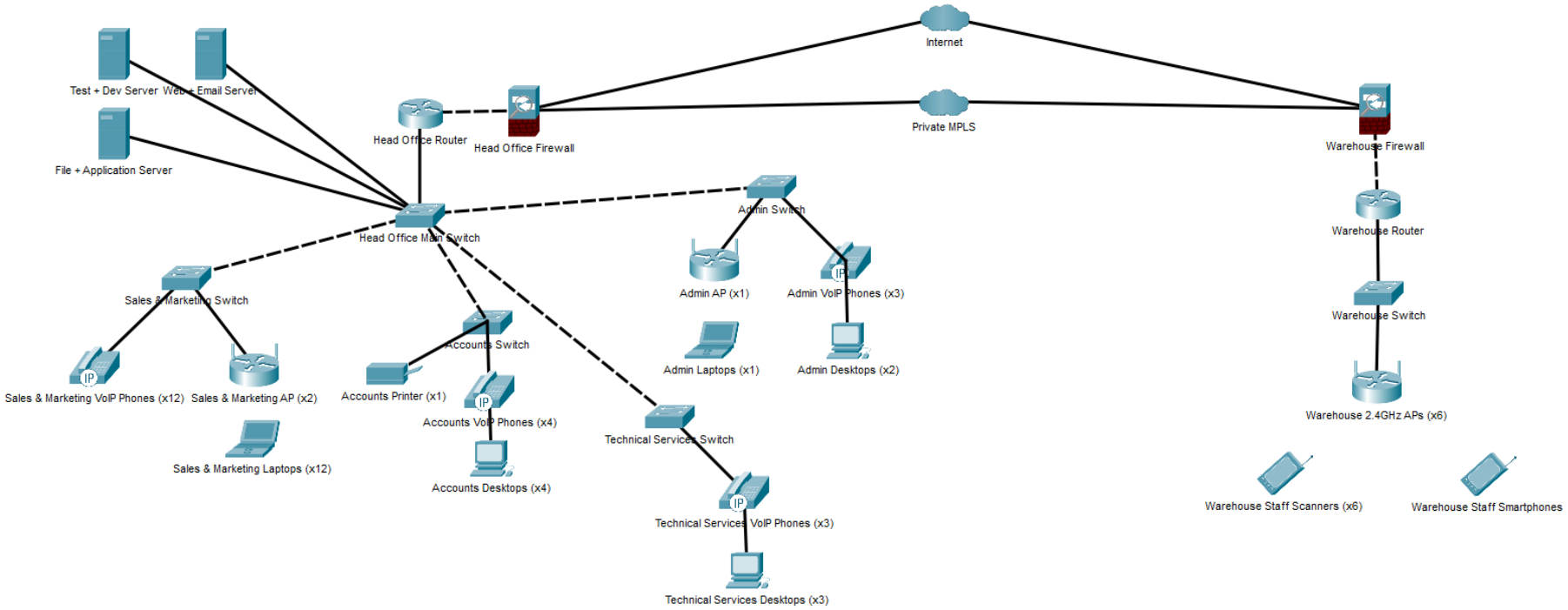
As Bancroft Systems is a smaller sized company, it can be assumed that the business will have a high level of flexibility when making a WAN solution work. Especially considering that no existing WAN infrastructure exists, Bancroft Systems can be considered a blank slate with the opportunity to implement the best possible fitting WAN solution. A virtual private network (VPN) is an application that runs on a server of which many clients can connect to. Communication between the VPN server and a client is encrypted nearly removing the risk of man-in-the-middle attacks and preventing hackers from sniffing and reading the packets. A VPN service will almost always include an authentication service, ensuring that only trusted users have access to the VPN. The VPN server will then act as a proxy between the user and the broader internet. Due to the flow of data with a VPN model, the VPN server can be trusted to access sensitive information and will act on behalf of an authenticated user. For example, an employee will login to the company's designated VPN service and will be able to perform their regular duties. This VPN can be used on any device, at any location, with any network. This ensures that the user remains compliant with any security rules and has access to their required resources to perform tasks. A VPN service is much less expensive than the proposed SD WAN solution and does not require an expensive MPLS connection from a telecommunications provider. The VPN can be used with any type of connection, such as high-speed broadband and the 4G/LTE network which have stronger value propositions. The VPN service is an exceptional solution for Bancroft Systems due to its simplicity, flexibility, ease of use, and its low cost.

Network Diagrams

Cloud Hosted VPN Service



SD WAN


Internet
Test + Dev Server
Web + Email Server
File + Application Server
Head Office Router
Head Office Firewall
Private MPLS
Warehouse Firewall
Head Office Main Switch
Admin Switch
Warehouse Router
Admin AP (x1)
Admin VoIP Phones (x3)
Sales & Marketing Switch
Warehouse Switch
Accounts Switch
Admin Laptops (x1)
Admin Desktops (x2)
Sales & Marketing VoIP Phones (x12)
Sales & Marketing AP (x2)
Accounts Printer (x1)
Accounts VoIP Phones (x4)
Warehouse 2.4GHz APs (x6)
Technical Services Switch
Sales & Marketing Laptops (x12)
Accounts Desktops (x4)
Warehouse Staff Scanners (x6)
Warehouse Staff Smartphones
Technical Services VoIP Phones (x3)
Technical Services Desktops (x3)

Conclusion

When designing an efficient and high value money networking solution, purchasing the best solutions on the market is not necessarily the answer. Bancroft Systems should first take the time to completely understand their business requirements, technical requirements, and potential network constraints. With this information, more appropriate decisions can be made to achieve the desired business requirements whilst managing identified constraints and keeping a low budget. Given the proposals within this report, Bancroft Systems will be able to achieve a network meeting their business requirements at an affordable cost.

Bibliography

[1]V. Beal, "What is 802.11 Wireless LAN Standards? | Webopedia", *Webopedia*, 2021. [Online]. Available: https://www.webopedia.com/definitions/802-11/. [Accessed: 14- Jan- 2022].

[2]"Wondering how your WiFi works? Here's how", *ACT Bengaluru*, 2020. [Online]. Available: https://www.actcorp.in/blog/what-is-wifi-and-how-it-works. [Accessed: 14- Jan- 2022].

[3]J. Lucas, "What Is Electromagnetic Radiation?", *livescience.com*, 2015. [Online]. Available: https://www.livescience.com/38169-electromagnetism.html. [Accessed: 14- Jan- 2022].

[4]"2400-2483.5 MHz (4 W)", *R-spectrum.com.au*, 2022. [Online]. Available: https://r-spectrum.com.au/resources/countries-nations/australia/wireless-bands/2400-24835-mhz-4-w. [Accessed: 14- Jan- 2022].

[5]"The differences between 2.4GHz and 5GHz Wireless | TP-Link", *Tp-link.com*, 2013. [Online]. Available: https://www.tp-link.com/us/support/faq/499/. [Accessed: 14- Jan- 2022].

[6]"Datto Networking: Which WiFi channels should I use?", *Help.datto.com*, 2021. [Online]. Available: https://help.datto.com/s/article/KB115005589863. [Accessed: 14- Jan- 2022].

[7]D. Zomaya, "When to Use 802.11 a, b, g, b, nc: WiFi Standards", *CBT Nuggets Blog*, 2021. [Online]. Available: https://www.cbtnuggets.com/blog/technology/networking/when-to-use-802-11-a-b-g-b-nc-wifi-standards. [Accessed: 14- Jan- 2022].

[8]"Half duplex radio vs Full duplex radio", *Rfwireless-world.com*, 2022. [Online]. Available: https://www.rfwireless-world.com/Terminology/Half-duplex-radio-vs-Full-duplex-radio.html. [Accessed: 14- Jan- 2022].

[9]"CSMA/CA: definition and explanation of the method", *IONOS Digital Guide*. [Online]. Available: https://www.ionos.com/digitalguide/server/know-how/csmaca-carrier-sense-multiple-access-with-collision-avoidance/. [Accessed: 14- Jan- 2022].

[10]"What is 802.11ax (Wi-Fi 6)? New Wi-Fi Standard | Extreme Networks - Extreme Networks", *Extreme Networks*. [Online]. Available: https://www.extremenetworks.com/wifi6/what-is-80211ax/. [Accessed: 14- Jan- 2022].

[11]"2.4 GHz vs. 5 GHz WiFi", *Centurylink.com*. [Online]. Available: https://www.centurylink.com/home/help/internet/wireless/which-frequency-should-you-use.html. [Accessed: 14- Jan- 2022].

[12]"What Is a Next-Generation Firewall (NGFW)?", *Cisco*. [Online]. Available: https://www.cisco.com/c/en_au/products/security/firewalls/what-is-a-next-generation-firewall.html. [Accessed: 14- Jan- 2022].

[13]"What Is Signature-Based Malware Detection?", *Logix Consulting Managed IT Support Services Seattle*, 2020. [Online]. Available: https://www.logixconsulting.com/2020/12/15/what-is-signature-based-malware-detection/. [Accessed: 14- Jan- 2022].

[14]R. Sobers, "134 Cybersecurity Statistics and Trends for 2021", *Varonis.com*, 2021. [Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics. [Accessed: 14- Jan- 2022].

[15]"What is phishing | Attack techniques & scam examples | Imperva", *Imperva*. [Online]. Available: https://www.imperva.com/learn/application-security/phishing-attack-scam/. [Accessed: 14- Jan- 2022].

[16]V. Onut, C. Lee and L. Kessem, "Phishing Attacks Are Top Cyber Crime Threat, Easier Than Ever to Create and Deploy", *Security Intelligence*, 2021. [Online]. Available: https://securityintelligence.com/posts/phishing-attacks-top-cyber-threat-create-deploy/. [Accessed: 14- Jan- 2022].

[17]A. Chugh, "What is the 'Great Resignation?' An expert explains", *World Economic Forum*, 2021. [Online]. Available: https://www.weforum.org/agenda/2021/11/what-is-the-great-resignation-and-what-can-we-learn-from-it/. [Accessed: 14- Jan- 2022].