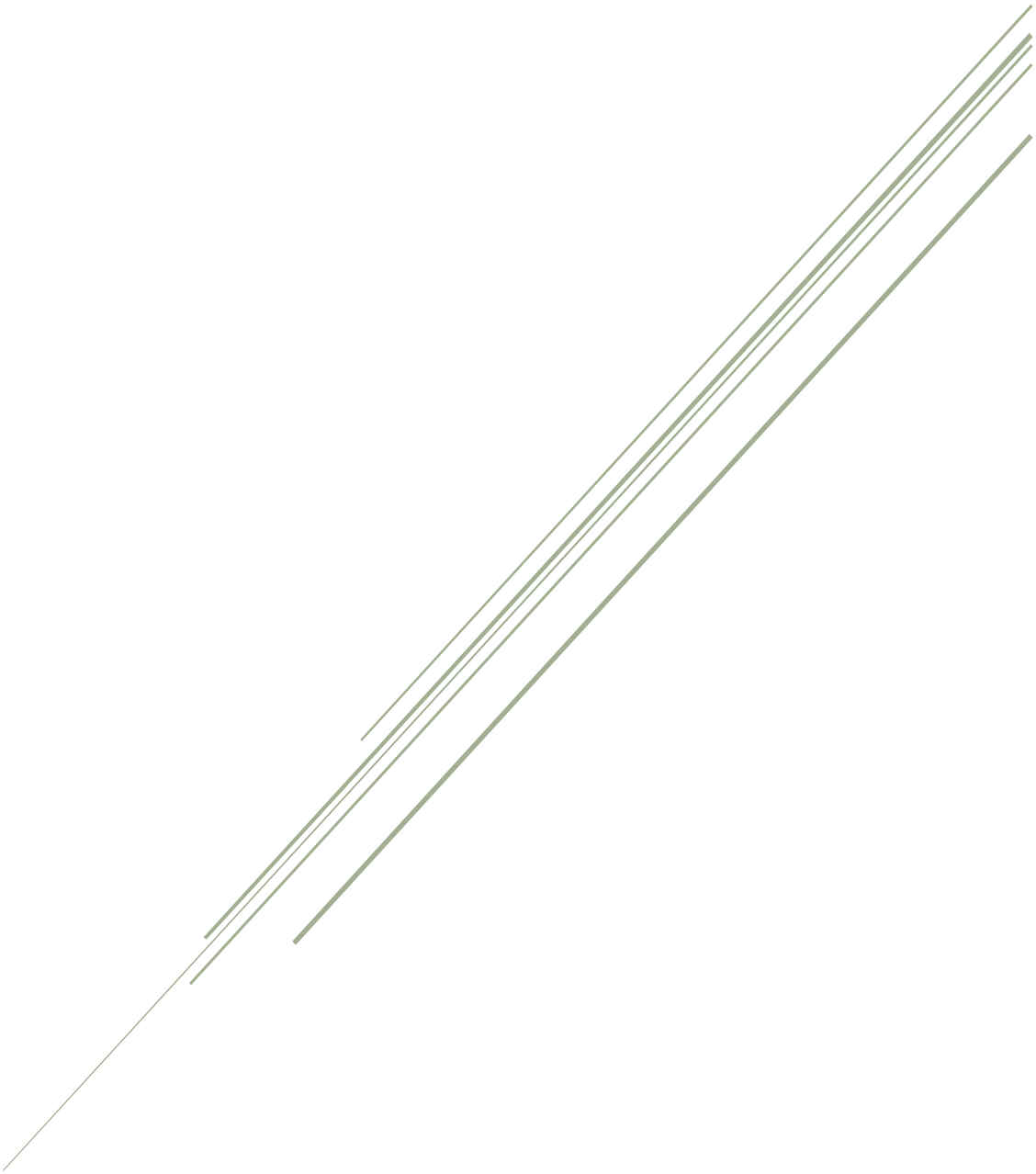
ASSIGNMENT 2

Rajiv Mehta - 45433062



Macquarie University
Data Communications

WAN Setup Choices

Option 1. Packet-Switched Network via an Ethernet Cable

The first option for connecting Mike's Soft's network and LockedIn Services network is to create a 'Packet-Switched Network' or PSN between the two companies via an ethernet cable connecting the routers from each WAN. [1] In a packet-switched network, data is transferred between nodes/computers through the breaking down of data into small packets. These packets carry the data through the network to the required destination via the physical layer i.e. the ethernet cable connecting the WANs and cables from routers and switches to computers. This method of networking allows for increased efficiency in data transfer as PSN is connectionless, meaning that a circuit does not need to be set up a private connection before sending data, therefore, reducing the latency of transfer. In order for this process to work, pathways between the WAN's and all the nodes in each LAN need to be first initialised at first setup so the locations of all endpoints are recorded in routing tables, address tables, etc. This is so that packets have multiple pathways to travel destination nodes and in turn, also allows multiple packets to be sent over the network. Therefore, implementing this method to create a WAN is a great option due to its connectionless nature and simple setup by just connecting the routers via an ethernet cable.

Security

This method of connecting the WAN's of each companies respective networks provides a good level of security within the network when communicating within the network. For starters, as the packets are being sent through a wired connection through the network rather than through a wireless method, external users can't access the data unless they are also physically connected to the network. This means that securing the data transfer over the network is easier as it would just involve making sure that anyone without proper authority cannot access the network via the endpoints. [2]Also, if using this method for extra security the business can easily implement a MAC address filter which only certain computers to access the network which would also help prevent unauthorised access to the network [3]. A certain problem that can arise by using an ethernet cable to connect the WAN networks and that is that packets retrieved from the internet via the routers can reach more devices and cause damage to more endpoints if malicious software is introduced into the system. For instance, if a 'Trojan horse' enters the system via the router with the intent of being able to access user systems, then the malware has a chance to affect all the systems from both WAN networks which could cause devastating effects for the business. Though, other security such as firewall can prevent this from happening so the security that a packet-switch network via an ethernet cable is still an efficient choice when considering how to create a wide area network.

Capital & Operational Expenditure

In terms of capital expenditure, the costs for setting up a wired packet-switch network is quite low. As the local area networks have already been set up prior, the only capital costs would be buying the ethernet cable, installing it within the building itself and potential repeaters if the ethernet cable is greater than 100m. Though, installing wiring in a building can be quite expensive the benefits outweigh the cost in this scenario as if done correctly it will provide security to the network and it can also reduce the long-term costs as the business does not have to pay a fee every time they want to use a shared ethernet cable like in circuit-switched networks.

Operational expenditure for the packet-switched network connected via an ethernet cable can be quite costly in terms of operational efficiency on the network speed. [3]For instance, when a packet from Mike's soft network needs to be sent to the LockedIn Services network, the packets can take many different paths to reach its destination. This means that the transfer of information can be slow in terms of speed and in turn, lowers the efficiency of the network. Also, as the packets are sent in small bursts, meaning that multiple packets are sent to transfer all the data, if even one of the packets become delayed, lost or corrupted then all the data has to be recent from the computer causing large delays. Even though this can occur, this method of setup does have an advantage in this regard, if the data does become lost, delayed or corrupted then the receiving computer knows exactly where the information is coming from and can request for the data to be resent without having to search the entire network for it.

Option 2. Implementing a Virtual Private Network

Another option for connecting the two local area networks would be to create a virtual private network (VPN) in order to create a wide area network. [4]A VPN is a system that many businesses use to encrypt their network when accessing the internet. This means that any packet of data that is being sent over the internet has another layer of protection from hackers and anyone who is trying to trace where the information is coming from. This works by having a router connect to a server outside of the business, mainly in another region/country via a private tunnel rather than the businesses internet service provider (ISP). This server then browses the internet for the information you are after meaning that anyone who is following the packet will just be able to trace it back to the server rather than the private network of the business. The packets that are sent and received are given an extra layer of security through this method as they undergo a process of encapsulation when travelling through the VPN tunnel. There are three main types of VPN, in the case of connecting the two networks to make a new WAN for the entire business, the businesses in this situation would set up an 'intranet-based' VPN which allows for virtual paths to be created for each end-node, which allows for packets to be sent from one LAN to the other as all the pathways are already logically mapped out.

Security

In terms of security, a virtual private network provides excellent security for the business when transferring data from network to network. [5] Firstly, as described earlier when sending packets through to the other network or accessing the internet, all packets are encapsulated when travelling to outside server. This means that when it reaches information such as source address, carried data, etc are all encrypted and can't be accessed by anyone using the public server or the internet, meaning that all private data is protected until it is back in the business network and at the destination address. Also as the network location and information is encrypted/hidden it is harder for hackers to try and access the system via the internet as the location and the packets are seen as just normal packets flowing through the internet. [6]Though, there are also potential risks with using a VPN. For instance, if the VPN provider the business has chosen does not set up their server correctly then the business is at risk of data leaks, which could lead to tracking of the business network and potential hacker and malware attacks. Though, even if the business does choose a poor VPN provider and malware like a Trojan Horse is in the system, the whole network is not at risk as the connections between the LANs are wireless. Therefore, the security VPN provides makes it a great option for merging the LAN's of each respective company.

Capital & Operational Expenditure

In terms of capital expenditure, the cost for a VPN is almost cost-free depending on the routers that both companies have. If the routers that both companies currently have support VPN, then the business will not have to buy new routers which reduces the costs for implementing a VPN, else the costs do raise. Also hiring a network engineer/team to initially set up the VPN can also be quite costly as well as having to replace all the IP addresses for the network as the VPN tunnel requires that the IP addresses fall within a certain range in order to access the tunnel.

[5]In terms of operational expenditure, implementing a VPN has a very high operational cost. This is due to the subscriptions that need to be constantly paid for VPN. Depending on the provider these costs can vary. Also if there is a problem with the business network due to a data leak which has allowed malware to affect computers then having to replace or repair these systems will cost large sums of money. Also if the company decides that it wants to expand its business more and needs to implement a new LAN, then it can easily do so but would also require buying more assets to make sure that it can access the other networks securely.

Overall Comparison

Both implementing a packet-switched network and implementing a VPN are both viable options for connecting the two networks. In terms of security, both methods implement different security methods to protect the network with the packet-switched having a heavy reliance on protecting the data by making it almost impossible to access the network without being plugged in via an endpoint and VPN relying on encrypting its data while it travels through the internet. upgrading of equipment to meet demand the

operational cost can be seen as relatively high in comparison. Capital expenditure for both methods can be quite costly especially for packet-switching as it requires having to install an ethernet cable to run through a building to the other network, which if done in the walls will require specialist workers such as electricians. Operational costs, on the other hand, are costly to both options but in different ways. In terms of the packet-switching, there are large delays in terms of packet travel time and loss, delay and corruption of packets which could all cause delays in the network. VPN has a monetary operational cost associated with it as it requires paid subscriptions and maintenance. Though, if the costs are managed well both options are a viable choice in connecting the two WAN networks.

Backbone network

The two local area networks being connected will cause initial problems on employees/users being able to access the right data from the right servers i.e. business accountants should be able to access the accounting records from both companies but the software developers should not be able to access these servers. To fix this problem the business will need to implement three changes to the network.

Switching to a private network

Currently, both Mike's Soft and LockedIn Services operate under a public internet protocol (IP) addresses. This current network can cause many problems in the security of the business as basically anyone can access the data in the servers. Any hacker would be able to enter the system and plant malware which could break the current network or even worse a hacker could steal information which could then be sold to a rival business. This would then let the rival see how the business is operating and make strategic decisions of their own to counteract Mike's Soft business, which could lead to business decline and failure. To stop this from happening it is paramount that Mike's Soft switches from its public network and obtain a new private network.

With this new private network, it will create a new sense of security within the network. Firstly, hackers and any unauthorised personal who would try and access the network would find it very difficult to find and get into the network. Also when using either of the options discussed above for connecting the networks, having a private network increases the overall security for when having a wired connection as hackers will have a hard time accessing the network from the internet and in turn, will have to access the network via the physical location of the business. This also helps with the VPN option, because if the packets/logs in the external server are breached, then the hackers will still require time to decipher the actual network it originated from and in turn, give the business time to change/secure their network.

Subnetting the private network

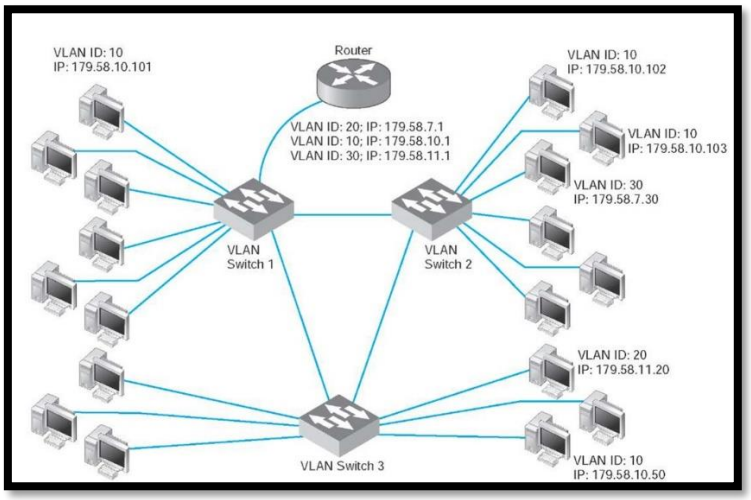
The first change involves obtaining a new private network for the business. With this new network, the business can subnet the network into smaller parts and assign each subnet to a certain team/department. This would not just separate and organise the endpoint addresses of the business but it also helps set up the VPN option for connecting the LANs as mentioned in the previous section. As the business is required to create subnets, choosing the subnet class is also important. [7]The business could opt for a class A or class B option in this case. Both of these types have unique advantages, for instance, class A is a good option as if the business decides to expand in the future, it will not need to replace the network as it class A allows for a large number of hosts per subnet to be created due to the fact that the network identification only take 8 bits from the available 32 bits. Though, a class B network can be a better fit then class A as it allows the business to make more subnets at the expense of the number of hosts per subnet which could be beneficial if the business were ever to expand the type of service it provides when expanding. Therefore, both subnet classes are an option for the business and choosing which will depend on the strategic plan for the business.

Virtual Local Area Networks

Step three and the final change to the network would be to implement a virtual local area network (VLAN). At the current stage in the merging of the businesses, each business is still currently located on different floors of the building and this could continue to be the case for the business for a very long time. This means

that accountants could be on two different floors and require access to the same server. To combat this problem, the business should implement VLANs. A VLAN is a method of setting up the network so that certain endpoints are a part of the same LAN. This method of setting up the network easily segregates each function of the business without having to physically move staff and endpoints around so that they can access the right information for their job. It does this by assigning ports on a switch to various virtual LANs so that when data is requested/sent through the switches will send it directly to the LAN if the LAN has the proper authority to access it.

Various types of VLANs that exist, each achieving a similar result but in different ways. In terms of this Mike's Soft, the use of a multi-switch IP based VLAN is the best option for the business. The way a multi-switched IP based LAN works is that first virtual LANs are created by specifying which IP addresses in the network are connected to which department as seen in figure 1. The switches then create switch tables and stores the ports of each device and there IP address. [8]This segments the access to users for certain networks. As the switches operate at layer-3, it reads the source and destination address of packets and if those are not a part of the same VLAN then the packet will not be able to go the destination address. This means that any department cannot access the server of another department unless given the correct authority i.e. joining the VLAN of the department they are trying to access. Another advantage of this method, is that if the business wants to expand its business, then all the business would have to do is to add connections at the switches, and as it's a multi-switch setup, if the number of ports on the switches runs out then connecting a new switch can be done as different switches can be used to connect to the same VLAN.



[13]Figure 1. Example of multi-switched IP

Implementing a VLAN does come with setup costs and problems for the business in the future. Firstly due to the VLAN operating through switches at layer-3, the switches have to open up every packet and send the packet through to the right destination which in turn, slows down the speed of the network considerably. Also if the business decides that it wants to expand the business to have more endpoints/hosts, if the number of ports runs out, then the business will have to buy more switches and cables while also having to update the network to allow for the right data to be accessed to the right authorisation. Though, the negatives can be quite extreme the positives of using an IP-based VLAN over the other types like Port-based can be quite inflexible or cost-heavy which could impact a growing business like Mike's Soft in a negative way.

Securing the Network

Securing the network is an important step that needs to be undertaken when merging Mike's Soft and LockedIn Services. As a new network is set up, updates to security and addition of new security is paramount for protecting business secrets form hackers and any potential threats. In order to do add security to the network the business should implement the following for security.

Firewalls

The first thing that needs to be implemented into the network is firewalls. [9]A firewall is a system that is implemented into a network either through software or hardware that prevents the unauthorised access from users on the internet to the private network. To achieve this, firewalls check each individual packet that comes in and out of the network and checks if the packets are safe to enter the network based on certain rules defined by the configuration of the firewall. Security is achieved by using combinations of different types of firewalls. For example:

- [10]Packet Filter Firewall: In packet filtering, the firewall analyses each packet that comes through the internet against a set of filters. These filters are defined by the business and if it does get stopped by a filter then the packet is blocked from entering the system.
- [9]Application Level Firewall: Application-level firewalls when implemented act as a gateway for when the network wants to access the internet. What this means is that the firewall hides the true network address so that when a packet that coming out of the network is requesting data, the firewall will edit the packet so that the true network address is unknown. Then when the data, that has been requested tries to enter the system, the firewall edits the packet with the original source and destination address.
- [11]Stateful Inspection Firewall: A stateful inspection firewall is very similar to a packet filter firewall except that the filter is dynamic. This means that the filter changes depending on the state and context of the network and packets. As an example, if a packet tries to enter the network, the firewall checks to see if the packet has a matching known active connection. If it does then the packet is allowed straight through the network which in turn, is a very fast process. Though, if not then the firewall does a check to see if the packet matches to any of the policies that allow it to pass through to the network, and at the end will either discard or add the packet to the flow table.

By using a combination of these types of firewall there are many benefits that are brought to protecting the business network. [9] [10] [11] Firstly with the use of packet filtering, due to the packets being checked by the firewall at the router, packets, in theory, do not have to be checked throughout the network speeding up the network and reducing the cost of having to buy additional security in the network. Though, by using a packet-filter firewall, each packet has to be analysed against known commands meaning that it will create latency when trying to receive data from the internet. Therefore, a Stateful Inspection firewall could be implemented as well so that known packets do not have to be re-analysed and let straight into the network. Also by using an application-level firewall on top of the packet-filter firewall, the firewall acts like a VPN meaning that it keeps the network hidden making it harder for hackers to locate the network.

Though combing firewalls like these secure the network quite well, it is not perfect and can come with some serious negative side effects for the business. [9] [10] [11] The first negative is that cost of firewalls can be quite high depending on the level of security it provides. Another issue is that there is the potential for packets to be analysed incorrectly which could lead to one of two things. The first scenario is that if the packet is dangerous but the firewall does not deem it as so, then the business will have malware travelling through the network which could cause serious problems for the business. The second scenario is that if the packet is safe to enter the network but the firewall does not allow it, then nobody in the network will be able to access that information leading to business inefficiencies. The last type of issue with implementing these firewalls is memory. As firewalls such as the stateful inspection firewall are dynamic, they require memory of patterns within packets in order to reduce delay when allowing traffic into the network. As a result, if the memory becomes full then the business will have to pay more to buy more storage and in turn, increase business costs. Though, as there are many negatives, the need for firewalls to protect the network outweigh the costs accompanied by them as they protect the network from external users.

Intrusion Detection Systems

Another security measure that could be implemented into the network would be an intrusion detection system (IDS). [12]An IDS is used to analyse packets that are already in the network to check for potential malware and unauthorised users. An IDS is implemented through hardware so when a packet is passed through it, the IDS analyses the packet against patterns that the network has deemed to be unsafe. Then if the packet is seen

to have a strange pattern that is unknown to the network, the IDS doesn't stop the packet but alerts the network and end-users that malware has potentially entered the system and that precautionary methods should be implemented to resecure the network. This is beneficial piece of security as it re-analyses traffic that has passed through the firewall and is inside the network, which means that if the firewall didn't pick up the malware as bad and is sent into the network then the malware will be reanalysed increasing the chances of detection. The negatives to implementing this can be quite detrimental. Outside of the negative impacts to the network speed and that it will cost the business to implement an IDS. Another important problem can arise is when the IDS analyses a perfectly fine packet as a problem and alerts the network of malware. This can cause the business to take measures and in turn, cause the business to stop operating until the problem has been fixed costing the business both time and money.

User Authentication

Another key security system that would need to be implemented into the network would be user-authentication. User authentication is the system that the business puts into place in order to verify that the users who are trying to access the network are authorised. To do this the business can implement various forms of authentication such as passwords to enter the network and allowable attempts at logging in, placing time frames for when the network can be accessed so nobody can access it after business hours, security on-site for the business to check everyone who enters the building and verify that they are authorised. All these methods of authorising users benefit the business in many ways. First with onsite security, unauthorised users will have a hard time trying to access the private network via a wired connection as there is security checking the building and in turn, reducing the chances of this happening become next to impossible. Even if the hacker did manage to get past security and they tried to access the network from one of the computers, then they would be blocked by network and endpoint passwords making the chances of them being able to access the network even smaller. Implementing this kind of security does come with extra costs to the business as do all other security implementations, the costs can be reduced significantly as the cost of physical security for the building would be shared between all the business operating in the building.

Additional Servers

The addition of extra servers into the network would be very beneficial for backing up the information of the network. It is important to have these servers in case the network is subjected to potential malware that was missed by the other security measures. For instance, if a virus enters the network and manages to reach a server or a host, then the information on those servers could be damaged and modified. By having these files backed up by another server, the chances of losing all of the businesses data is reduced and in turn is very beneficial for securing the network. The negative to implementing this is that more servers mean additional costs but also another potential way for hackers to steal information from the business. Though, the chances of this occurring are small therefore, having a backup of business data is paramount.

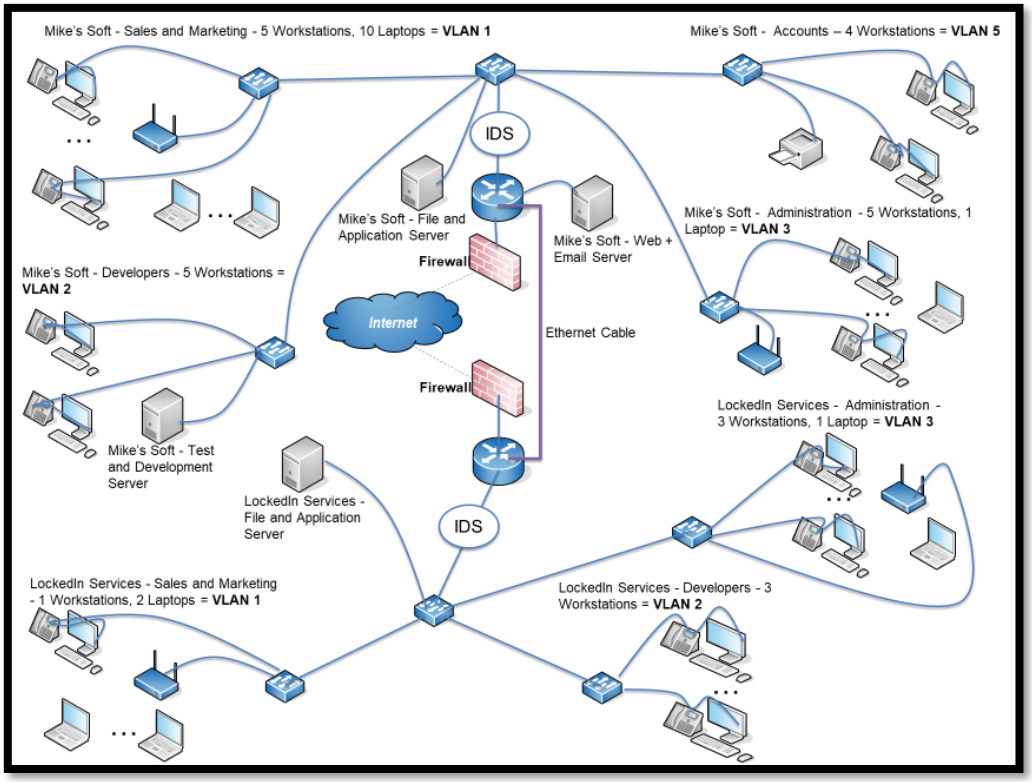
Network Diagrams

Assumptions and Key Notes:

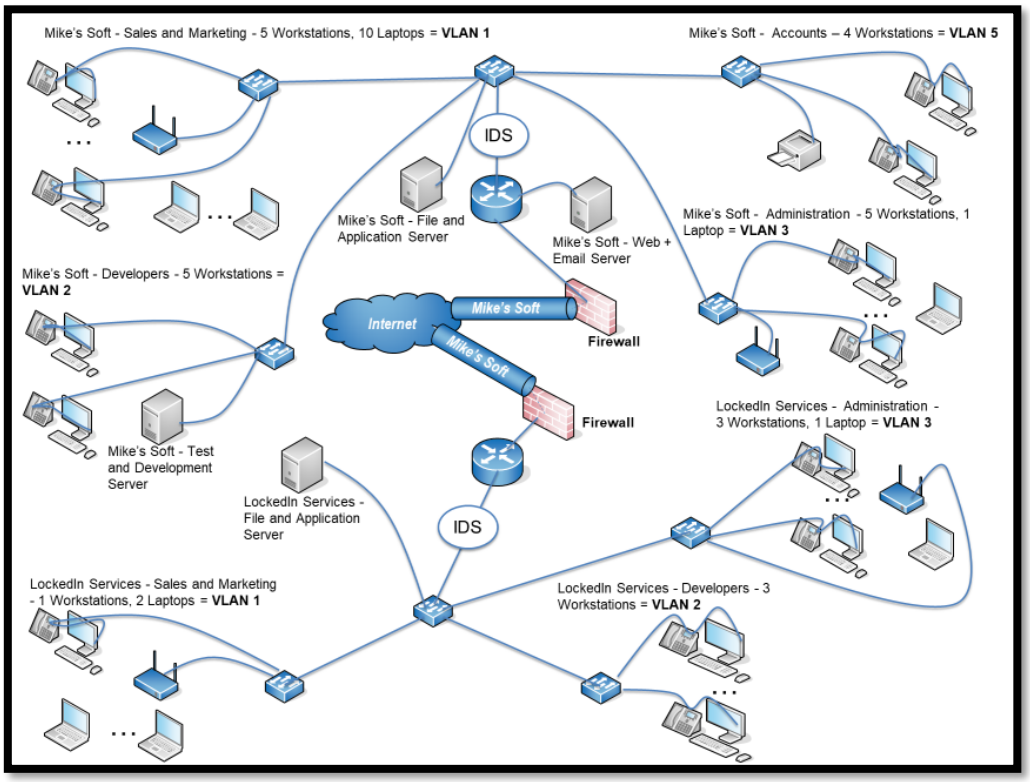
- The subnet class chosen by the business is a class B and 8 subnets have been created to fill the first 5 VLANs. The new network that Mike's Soft obtains is: 10.5.0.0 /16. The host ranges are given below:
    - VLAN 1 = 10.5.0.0 – 10.5.31.255
    - VLAN 2 = 10.5.32.0 - 10.5.63.255
    - VLAN 3 = 10.5.64.0 - 10.5.95.255
    - VLAN 4 = 10.5.96.0 - 10.5.127.255
    - VLAN 5 = 10.5.128.0 - 10.5.159.255
- IDS = Intrusion detection system
- Firewalls are usually built in the router but for this logical diagram it assumed that the firewall is before the router for clarity.

- Additional Servers are not included in the diagram to make it easier to look at. It can be assumed that where a server is located, a backup server is in the same location.

Packet-Switched Network via an Ethernet Cable



Virtual Private Network



References

[1] L. Copeland, “Packet-Switched vs. Circuit-Switched Networks,” COMPUTERWORLD, 20 March 2000. [Online]. Available: https://www.computerworld.com/article/2593382/networking-packet-switched-vs-circuit-switched-networks.html. [Accessed 26 May 2020].

[2] V. Bajaj, “MAC Filtering in Computer Network,” GeeksForGeeks, unknown unknown unknown. [Online]. Available: https://www.geeksforgeeks.org/mac-filtering-in-computer-network/?ref=lbp. [Accessed 26 May 2020].

[3] B. Mitchell, “How Packet Switching Works on Computer Networks,” Lifewire, 18 July 2-19. [Online]. Available: https://www.lifewire.com/packet-switching-on-computer-networks-817938. [Accessed 26 May 2020].

[4] C. P. &. S. C. JEFF TYSON, “How a VPN (Virtual Private Network) Works,” howstuffwork, 14 April 2011. [Online]. Available: https://computer.howstuffworks.com/vpn3.htm. [Accessed 27 May 26].

[5] S. Symanovich, “What is a VPN?,” Norton, Unknown Unknown Unknown. [Online]. Available: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html. [Accessed 26 May 2020].

[6] T. Mocan, “The Top 8 VPN Security Risks (What to Look Out for),” CactusVPN, 21 October 2019. [Online]. Available: https://www.cactusvpn.com/vpn/vpn-security-risks/. [Accessed 26 May 2020].

[7] SolarWinds MSP, “An Overview of Subnet Classes,” SolarWinds MSP, 5 June 2019. [Online]. Available: https://www.solarwindsmsp.com/blog/overview-of-subnet-classes. [Accessed 30 5 2020].

[8] L. Rathnam, “WHAT IS A LAYER 3 SWITCH AND WHY WOULD YOUR NETWORK NEED IT?,” TechGenix, 5 October 2018. [Online]. Available: http://techgenix.com/layer-3-switch/. [Accessed 30 May 2020].

[9] Indiana University, “About firewalls,” Indiana University, 15 February 2019. [Online]. Available: https://kb.iu.edu/d/aoru#:~:text=A%20firewall%20is%20a%20system,to%20the%20internet%2C%20especially%20intranets.. [Accessed 31 May 2020].

[10] J. Tyson, “How Firewalls Work,” howstuffworks, 24 October 2000. [Online]. Available: https://computer.howstuffworks.com/firewall1.htm#:~:text=A%20firewall%20is%20simply%20a,it%20is%20not%20allowed%20through.&text=With%20a%20firewall%20in%20place%2C%20the%20landscape%20is%20much%20different.. [Accessed 31 May 2020].

[11] R. MISHRA, “UNDERSTANDING FIREWALLS THROUGH THE LENS OF STATEFUL PROTOCOL INSPECTION,” Illum I/O, 5 December 2019. [Online]. Available: https://www.illumio.com/blog/firewall-stateful-inspection. [Accessed 31 May 2020].

[12] M. K. Pratt, “What is an intrusion detection system? How an IDS spots threats,” CSO, 19 February 2018. [Online]. Available: https://www.csoonline.com/article/3255632/what-is-an-intrusion-detection-system-how-an-ids-spots-threats.html. [Accessed 31 May 2020].

[13] Unknown, “Backbone network architectures (Data Communications and Networking) Part 2,” what-when-how, Unknown Unknown Unknown. [Online]. Available: http://what-when-how.com/data-communications-and-networking/backbone-network-architectures-data-communications-and-networking-part-2/. [Accessed 30 May 2020].