COMP1002

Assessment 2: Report

Contents

Introduction

Network infrastructure is an important consideration of any business when they settle into a new building/environment – the way that the network is set up will determine how efficiently and effectively the business can function. Everything within the business is fully reliant on this network being operational (Do you know the importance of your Network Infrastructure?, 2018). Important factors that must be considered when designing a network can range from costs of equipment and installation to scalability. Networks should be of a sufficient capacity and provide security as well as fast speeds. Overall, the main importance of network infrastructure is reliability (Do you know the importance of your Network Infrastructure?, 2018) – an unreliable network can result in unwanted downtimes, decreases in productivity, and may even unintentionally expose vulnerabilities that can be taken advantage of in malicious ways.

So, why is this report being written? Plymouth Home Stores has outsourced their network infrastructure design onto the producer of this document. This document will testify and discuss several considerations, and ultimately advise a specific infrastructure that fulfils Plymouth Home Stores' requirements. To accomplish this, the report has been decomposed into the following sections:

- System Architecture
- Network Architecture
- Security Architecture
- Conclusion

Overall, by the end of this document, the reader will be expected to have an image of a design that attempts to consider the previously mentioned qualities as well as understand how the network will incorporate security features to protect Plymouth Home Stores' digital assets.

System Architecture

The design of a network is typically dependant on, and structured around, the business' requirements. In the case of Plymouth Home Stores, the network that this report will aim to build upon should therefore consider factors such as the size of the business, and from this the capacity of the network can be understood. Another requirement is the segregation of Admin functionality, Staff functionality and Guest functionality. Ideally, each type of user will have a different degree of Access Level (this will be further explored within Security Architecture).

This section of the report aims to explore the core infrastructure of the network – such as the appropriate technologies needed to build the network and the physical locations of these technologies. However, to realise which technologies are needed, an in-depth exploration of the networks requirements is needed.

One such goal for the Plymouth Home Stores HQ network is to be able to provide employees the functionality to communicate with external partners and branches. These communication formats can range from emails to multimedia web conferencing. As such, the network should be able to maintain a high bandwidth to provide better performance. Therefore, one such requirement is for the network to be able to handle high amounts of traffic. If not, then the efficiency of the system will create a bottleneck in the productivity of the staff – affecting PHS's day-to-day operations.

Another concern is that the network should provide redundancy. This means that if one core component of the system goes offline, the network can still operate through backup or secondary means. This will help eliminate unwanted downtime of the network in the case of a technological problem.

By understanding these requirements, one can infer that the Cisco Three Layer Hierarchy model best suits this network. The model provides the above benefits (performance and redundancy) as well as a few others such as (Cisco Three Layer / Three-tier Hierarchical Network Model, n.d.):

- Better network management
- Potential scalability

This model segments the network design into: Access, Distribution, and Core. To build this type of network, multiple switches are required to maintain the hierarchal design. As such the network becomes easily manageable. Switches would be physically located in all rooms where computers require a physical connection to receive access to the internet (such as via Ethernet cabling). On each floor of the HQ there would be a Wireless Access Point through which clients would be able to connect via Wi-Fi connections. Switches could generally be placed within comms cabinets within these rooms to prevent individuals from accidentally or intentionally sabotaging the devices and therefore taking devices off the network – this works because the cabinets can be locked.

The previously mentioned switches can be identified as the cheap, slower switches that build up the backbone of the Access layer. The switches used within the Core and Distribution layers would be much more sophisticated – such as through introducing Multilayer switches. Depending on the size of the HQ, PHS could further simplify the 3-layer hierarchy by combining both Core and Distribution layers – mostly applicable if the location is small. For a vast physical location that has multiple buildings, the Distribution switches would generally be separated across buildings. Each distribution switch would connect to each other to provide greater redundancy – multiple routes for data to take on the network can be discovered and therefore if one device goes down, the data can take another path to bypass the faulty equipment/issue.

Through VLAN technology, the network can be easily segmented as 'types' of users can be separated and grouped. This allows sales staff to be separated from admin staff. Generally, each type of user has different needs and therefore will not need to access the same resources as other users. This segmentation therefore provides role-based access control – preventing outsiders from infiltrating the network (VLAN network segmentation and security-chapter five [updated 2021] - Infosec Resources, 2021).

Finally, connecting to the Core switches will be the router that provides the network access to the Internet – therefore allowing clients to send data to external partners. This router essentially forward packets from the clients outwardly to the Internet – but also from the Internet to the clients. A range of technology that can be used to

ensure that these packets are not malicious will be identified within Security Architecture. This router will generally be located alongside the Core switches within an IT closet that is well ventilated.

Overall, the network will provide both Ethernet and Wi-Fi connectivity for users. Through accessing the network, they can send and receive data via the router – but also access the HQ's servers to retrieve any data that they might need. The switches within the network will be connected via Copper Crossover cables, whilst Straight Through cables will be regularly used elsewhere, such as when connecting PCs to switches or switches to routers.

Network Architecture

Further developing the requirements and details outlined above, this report will now portray a theorised design for the network. This design is logical and therefore does not fully base itself around physical constraints of the HQ, such as numerous buildings or room layouts. This section of the report will explain the design choices and also provide the subnetting calculations for the network.

Subnetting the network's IP address space has the additional benefit of making the network manageable through creating logical smaller networks within. PHS' network will be divided into the following subnets:

- Admin
- Sales
- Guest Wi-Fi
- Employee Wi-Fi
- Servers

The technicalities of each subnet can be found on the following page.

Isolation of each subnetwork within the network allows for network administrators to eaily manage the network as they can easily contain threats – users are also constrained to only being able to access what they require, nothing more. Valuable informaiton can therefore be protected.

As seen in the packet tracer file that accompanies this report, the network has four multilayer switches that build up the Core and Distribution backbone of the network. These switches are connected in a partial mesh topology configuration so that the network can be made redundant. These swithces are all Layer 3 switches. The Distribution layer switches are wired to the Layer 2 switches that make up the access layer. Each Layer 2 switch is wired to each Distribution switch.

Network: 17.1.7.0 / 24
Servers: 14

Admin

Specification	Value
Number of bits in the subnet	28
New IP mask (decimal)	255.255.255.240
Number of usable subnets	16
No. of usable hosts per subnet	14
Network address	17.1.7.144
First IP Host address	17.1.7.145
Last IP Host address	17.1.7.158

Sales

Specification	Value
Number of bits in the subnet	27
New IP mask (decimal)	255.255.255.224
Number of usable subnets	8
No. of usable hosts per subnet	30
Network address	17.1.7.64
First IP Host address	17.1.7.65
Last IP Host address	17.1.7.94

Guest Wi-Fi

Specification	Value
Number of bits in the subnet	27
New IP mask (decimal)	255.255.255.224
Number of usable subnets	8
No. of usable hosts per subnet	30
Network address	17.1.7.66
First IP Host address	17.1.7.67
Last IP Host address	17.1.7.126

Employee Wi-Fi

Specification	Value
Number of bits in the subnet	26
New IP mask (decimal)	255.255.255.192
Number of usable subnets	4
No. of usable hosts per subnet	62
Network address	17.1.7.0
First IP Host address	17.1.7.1
Last IP Host address	17.1.7.62

Servers

Specification	Value
Number of bits in the subnet	28
New IP mask (decimal)	255.255.255.240
Number of usable subnets	16
No. of usable hosts per subnet	14
Network address	17.1.7.128
First IP Host address	17.1.7.129
Last IP Host address	17.1.7.142

Security Architecture

Within this report it has previously been mentioned that Access Control will be used to constrain the access of users to only those with authorisation. Access Control will work via assigning each user within the business a username and a password – their accounts would be assigned to a specific VLAN so that they are segregated from other roles within the business. A strong password policy would need to be implemented, such as:

- Password length is greater than 6 characters
- Password contains a special character
- Password contains a number

Further procedures that PHS should implement are those that supplement the knowledge of their employees. Essentially, staff should be made aware of what effective passwords look like (such as not containing personally identifiable information). They should be further educated on different types of cyber attacks like phishing, scamming, and ways that hackers can get them to install malicious software – such as through email attachments.

Educating their personnel is an important factor in protecting high value assets as interpersonal attacks provide attackers an easy way to sabotage systems. One such case study (Phishing attacks: defending your organisation, 2018) reported that although most malicious emails can be stopped through email filtering technology, those that made it onto the system attempted to run malicious code. In these instances, the devices were protected by up-to-date software. From this study it can be inferred that there should also be a policy that indicates frequent software updates – which can be easily distributed through VLAN management software.

Procedures and services for staff to be able to report suspicious activity or phishing attempts should also be in place so that threats can be contained. However, if threats cannot be contained an Incident Response Plan should be followed. This is essentially a policy that dictates what each user within the system should do and outline the most suitable responses in case of specific emergencies.

Email filtering technology is an effective way of preventing suspicious emails from being received by users – likewise, firewalls work similarly but with data packets instead. Firewalls can be configured to block specific types of packets before they get into the network. Anti-viruses can be installed within each computer on the network and regularly run within downtime of the business' services to ensure that each device is free of malware. Administrators can use anti-virus software to know if malicious software has been installed then take countermeasures to remove it safely.

However, digital attacks are not the only way of attacking a network. The physical hardware of the network should be protected. Common threats include thievery or sabotage, as well as natural disasters (fire, flood etc.). Natural disasters can be mitigated by regularly making a backup of the network and storing it safely offsite. Likewise, the way the building is built and where the technology is physically located should be considered. Switches and routers should be stored within cabinets and comms rooms should be fully utilised. These cabinets and rooms can be locked via keypads or keys to prevent unauthorised access.

CCTV should also be implemented to keep watch over valuable hardware, such as IT closets. CCTV ensures that perpetrators can be found in the case of a malicious event. Furthermore, access to the HQ can be monitored via staff lanyards that have RFID chips – these provide physical access control to the building/specific rooms. Movement of staff throughout can be monitored, as well as the ability to keep non-staff members out of designated areas.

Conclusions

Overall, this report has examined the technology that PHS will be required to use to form their network, how to structure their network, and how to prevent their assets from being sabotaged. Rather than using flat file networks, they should use the CISCO Three Layer model as it ensures that the network can be appropriately scaled in the future, as well as providing greater manageability, which is one of the main problems of networks that are large in size. Administrators need to easily be able to diagnose issues within networks and potentially even shut parts down. With potentially hundreds or even thousands of devices to manage, the modularity and segmentation makes it much easier. A variety of technologies that provide this segmentation have been explored, such as: VLANS and subnets.

Overall, other network designs have limitations and are not designed in mind with expanding businesses – the Three Layer Hierarchal model is an exception. Implementing one of these structures has the potential limitation of reducing productivity, having a network that can not grow alongside the growth of the company, be weak to digital threats etc. However, most importantly, this reports theorised design includes redundancy. If one component fails, there are secondary means to use which keep the network operational. Without this redundancy, the company potentially loses their web services and as a direct result, they lose income.

References

Infosec Resources. 2021. VLAN network segmentation and security- chapter five [updated 2021] - Infosec Resources. [online] Available at: <https://resources.infosecinstitute.com/topic/vlan-network-chapter-5/>.

Remark Group. 2018. Do you know the importance of your Network Infrastructure?. [online] Available at: <https://www.remark-group.co.uk/industry-news/do-you-know-the-importance-of-your-network-infrastructure>.

Ncsc.gov.uk. 2018. Phishing attacks: defending your organisation. [online] Available at: <https://www.ncsc.gov.uk/guidance/phishing>.

Omnisecu.com. n.d. Cisco Three Layer / Three-tier Hierarchical Network Model. [online] Available at: <https://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php>.