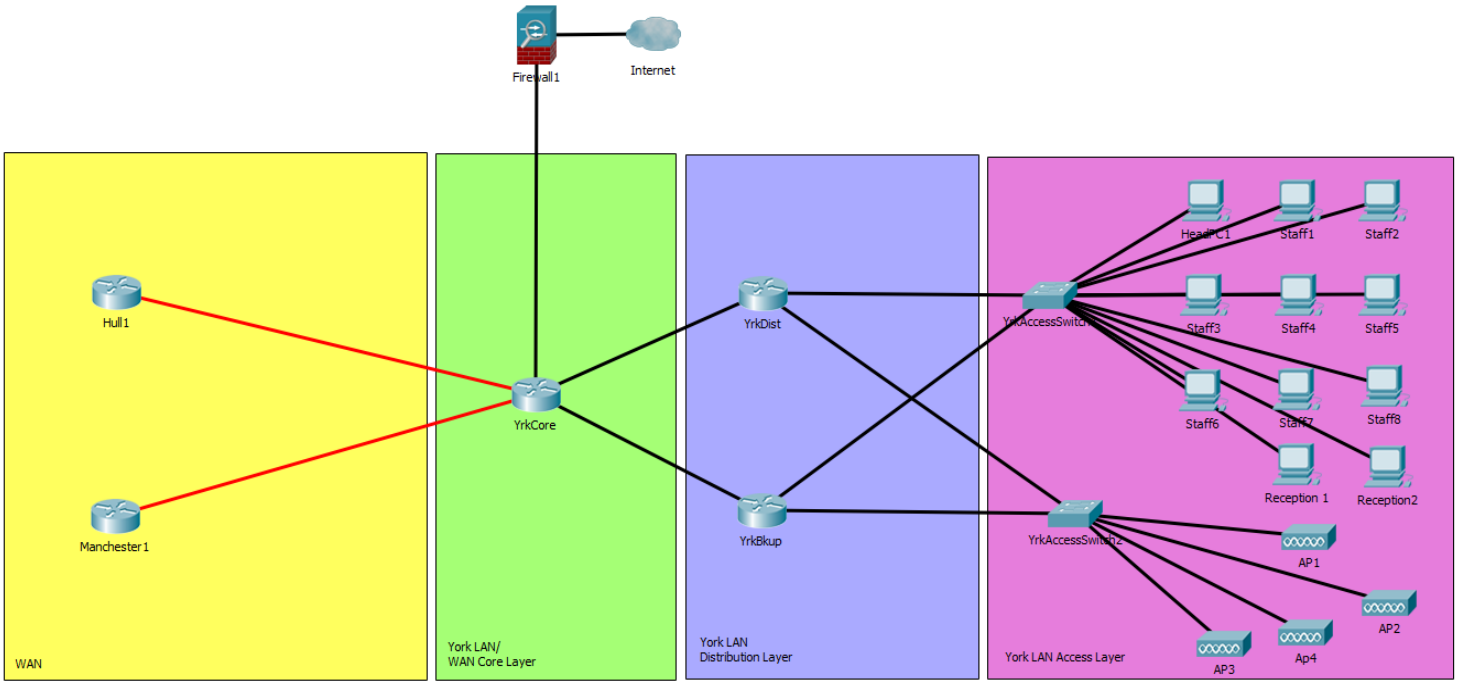
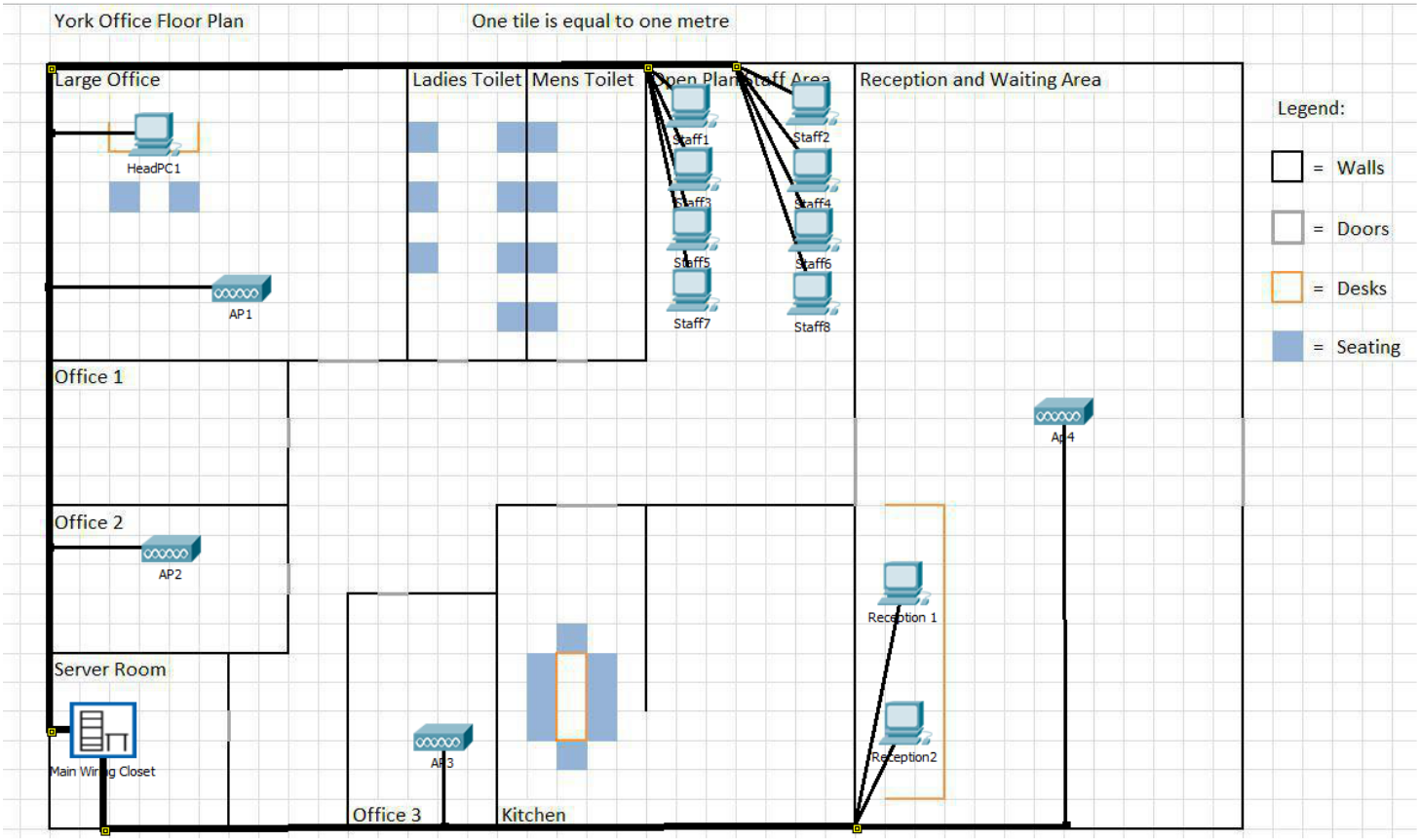
Logical Layout for York LAN and Company WAN



Physical Layout for York LAN



CMP2007M Networking Report

Network Layout:

When designing the network for the company network several factors were taken into consideration including data transfer rates, security needs, redundancy and cost. A hierarchical star topology was chosen in this case. “A hierarchical network design involves dividing the network into discrete layers” (,6), this is in opposition to a flat network which consists of only layer 2 switches with no higher-level devices connected. The hierarchical choice was made because more options would be given to the company for security and control than if a flat design was used. A star topology was decided on to allow for a cost effective centralised device to be used. This hierarchical design involves splitting a network into three layers; Access, Distribution and Core. The Core layer is usually the layer that runs most connections to WANs and so is optimized for performance and efficiency using expensive routers. This is connected to the distribution layer, the layer focussed on policies and virtual security. In this design the distribution layer has a backup device in case of failure which will be used as a secondary route for the network traffic unless the main device fails in which it will take over until the main can be replaced. This was not implemented in the core layer as it would be costly and the core router is supposed to be high end anyway and less prone to breakage. The Access layer focusses on providing services to end users, usually containing switches or Access Points.

The centralised core layer will be the layer that links all three LANs of each business into a WAN, this means much greater efficiency and cost reduction than if all three businesses had all three layers and the subsequent technicians to maintain them.

To cut down on cost for this hierarchical design the Distribution and Core layers could have been collapsed into a multi-layered switch, this would reduce functionality however and because it is not specified what the businesses produce or what services they provide it would be best to allow the design to be versatile.

Sub-netting:

The devices used in this system could be categorized into these distinct subnets: Offices, Staff, Wireless and WAN. These all have different numbers of devices but considering that the York building is the HQ it would be reasonable to assume it has the most network devices. The devices per subnet in the complete York LAN would be below thirty by a large margin but considering there is not enough data on the offices to know how many devices are contained within them thirty devices per subnet was chosen to be conservative. The sub-netting is shown below:

Subnet	Net ID	First	Last	Broadcast
1.Offices	0	1	30	31
2.Staff	32	33	62	63
3.Wireless	64	65	94	95
4.WAN	96	97	126	127
	128			

These subnets allow for a large increase in devices in the future, there are also four more subnets in case more are needed or the allocated subnets become full.

Security:

To secure the network a number of protections needed to be put into place, both software and hardware. The previously mentioned subnets would be a software solution that allows any network infection to be contained in only the specific subnet attacked and stop its spread because all devices are split up into their own smaller networks. VLANs are also a good use of software provided in switches, further separating the network into smaller virtual networks.

A hardware firewall will be set up between the internet and the rest of the system to protect the network from malicious programs coming through, to do this, rules are implemented. These are usually either rules to accept, reject or drop a connection dependant on its validity and the port it's being sent through. An example of these rules in the network would include Accepting inbound and outbound connections from port 80, which is of the html webpage type so the staff can access the internet.

Standards & Protocols:

To make sure the network runs efficiently certain protocols and standards need to be put in place.
The devices need to be connected with different cables depending on their location and mobility. All cabling in the LAN will be ethernet following the Category (CAT) 6 standard, this is most cost-effective choice for a business this size while still having fairly manoeuvrable cabling. The CAT 6 cables give 10 Gigabit per second speeds for up to 50 metres, this means the cabling can give that higher speed all the way through the York building and even if the cabling goes over this distance it still has the ability to go up to a theoretical maximum of 1Gbps for up to 100 metres, this is comparison to CAT 5e which while cheaper only has that 1Gbps speed theoretical maximum while also experiencing a lot more interference. The cabling could have used newer standards such as CAT 6A or CAT 7 but CAT 6A is nearly the same as CAT 6 apart from its increased thickness to improve on interference and increase the max distance for 10Gbps speeds, but also vastly reducing its flexibility, it is "better suited for industrial environments at a lower price point." (Mailheau, 2016). CAT 7 has only fairly recently come into use and so is expensive and although it boasts 100Gbps speeds at a distance of up to 15m it is only really used in larger networks.
The WAN cables use fibre optic connections, this is chosen over ethernet like that used in the LAN because it is much more effective and transferring data over longer distances such as the distances between the three offices, it is also more secure than ethernet cables because "information sent via fiber-optic cabling is much more difficult to intercept because light can't be read in the same way signals sent via copper cabling can be." (Bishop, 2013).
Once all cables connect the devices together a routing protocol is needed. The main choices are RIP, OSPF and EIGRP. RIP is quite useful in very small businesses where a handful of routers are used but not very useful when expanding past this number. EIGRP is better in this regard but is proprietary to Cisco and so would mean you are fully tied into their product which does not allow for much future flexibility, it is also a lot of overhead and uses a lot of resources. OSPF is the only Routing protocol that is both effective and flexible and so is much better suited for this network.

The four wireless access points attached to the LAN will use the IEEE 802.11ac standard to connect end user devices, this uses all of the standards that came previously, 802.11b, g and n. To give access over as much distance as possible the devices will use the 2.4GHz band rather than the 5GHz even if at lower speeds.

IP Addressing table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
Staff 1-8	NIC	192.168.1.33-40	255.255.255.224	192.168.4.1
HeadPC1	NIC	192.168.1.1	255.255.255.224	192.168.4.1
Reception 1-2	NIC	192.168.1.41-42	255.255.255.224	192.168.4.1
YrkAccessSwitch1	VLAN 1	192.168.4.11	255.255.255.0	192.168.4.1
YrkAccessSwitch2	VLAN 2	192.168.5.11	255.255.255.0	192.168.4.1
YrkDist	G0/0	192.168.4.1	255.255.255.0	N/A
	G1/0	192.168.5.1	255.255.255.0	N/A
	G2/0	192.168.6.1	255.255.255.0	N/A
YrkBkup	G0/0	192.168.4.2	255.255.255.0	N/A
	G1/0	192.168.5.2	255.255.255.0	N/A
	G2/0	192.168.6.2	255.255.255.0	N/A
YrkCore	G0/0	192.168.1.97	255.255.255.224	N/A
	G1/0	192.168.1.98	255.255.255.224	N/A
	G2/0	192.168.1.99	255.255.255.224	N/A
	G3/0	192.168.1.100	255.255.255.224	N/A
	G4/0	192.168.2.1	255.255.255.0	N/A
Hull1	G1/0	192.168.1.101	255.255.255.224	N/A
Manchester1	G1/0	192.168.1.102	255.255.255.224	N/A

CMP2007M Networking Threat Report

DDOS:

A DDOS (Distributed Denial of Service) attack is caused by several computer systems overloading the capability of a network. This is an attempt to "prevent legitimate users from accessing information or services" (D.).

Trojan Horse:

Trojan horses are malicious pieces of code that are disguised as legitimate. They focus on a user of a system to fall for the ruse and click on the folder or run the program that the malicious code lies within.

Rootkit:

Rootkits are software that attempts to stay undetectable on a computer

References:

Network Report:

http://ptgmedia.pearsoncmg.com/images/9781587133329/downloads/ch01.pdf

http://etutorials.org/Networking/Lan+switching+first-step/Chapter+10.+LAN+Switched+Network+Design/Flat+Network+Topology/

Bishop, E. (2013) *Ethernet vs. Fiber – Everything You Need to Know.* Available from https://www.business.org/services/internet/ethernet-vs-fiber-basics/ [accessed 17 April 2018]

Mailheau, R. (2016) *Demystifying Ethernet Types — Difference between Cat5e, Cat 6, and Cat7.* Available from https://planetechusa.com/blog/ethernet-different-ethernet-categories-cat3-vs-cat5e-vs-cat6-vs-cat6a-vs-cat7-vs-cat8/ [accessed 17 April 2018]

http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

https://technet.microsoft.com/en-us/library/cc700820.aspx

Network Threat Report:

United States Computer Emergency Readiness Team(2009) *Understanding Denial-of-Service Attacks.* Available at https://www.us-cert.gov/ncas/tips/ST04-015 [accessed 18 April 2018].

https://www.academia.edu/35511953/Spyware_and_Trojan_Horses

https://www.academia.edu/29724449/Digital_Warzone_An_Analysis_on_Behavior_Patterns_of_Trojan_Attacks

https://utica.edu/academic/institutes/ecii/publications/articles/EFE2FC4D-0B11-BC08-AD2958256F5E68F1.pdf

https://rd.springer.com/article/10.1007/s11416-007-0045-1

https://www.symantec.com/connect/blogs/handling-todays-tough-security-threats-rootkits

Daniel Dixon 16602092