Network and System Administration

ICA Part 1

Part 1

The first thing that I wanted to do to make sure that my assessment and therefore my plan is accurate is to find a reliable way of calculating the size of the buildings at Liverpool Hope university. A very reliable way of finding information on building dimensions is by using google maps and its measure feature, which is why I'll be using this as my main source of information when it comes to area, length, width and floors. I should be able to go into street view to find out floor numbers on most buildings and if I can do this the data collected will be very accurate.

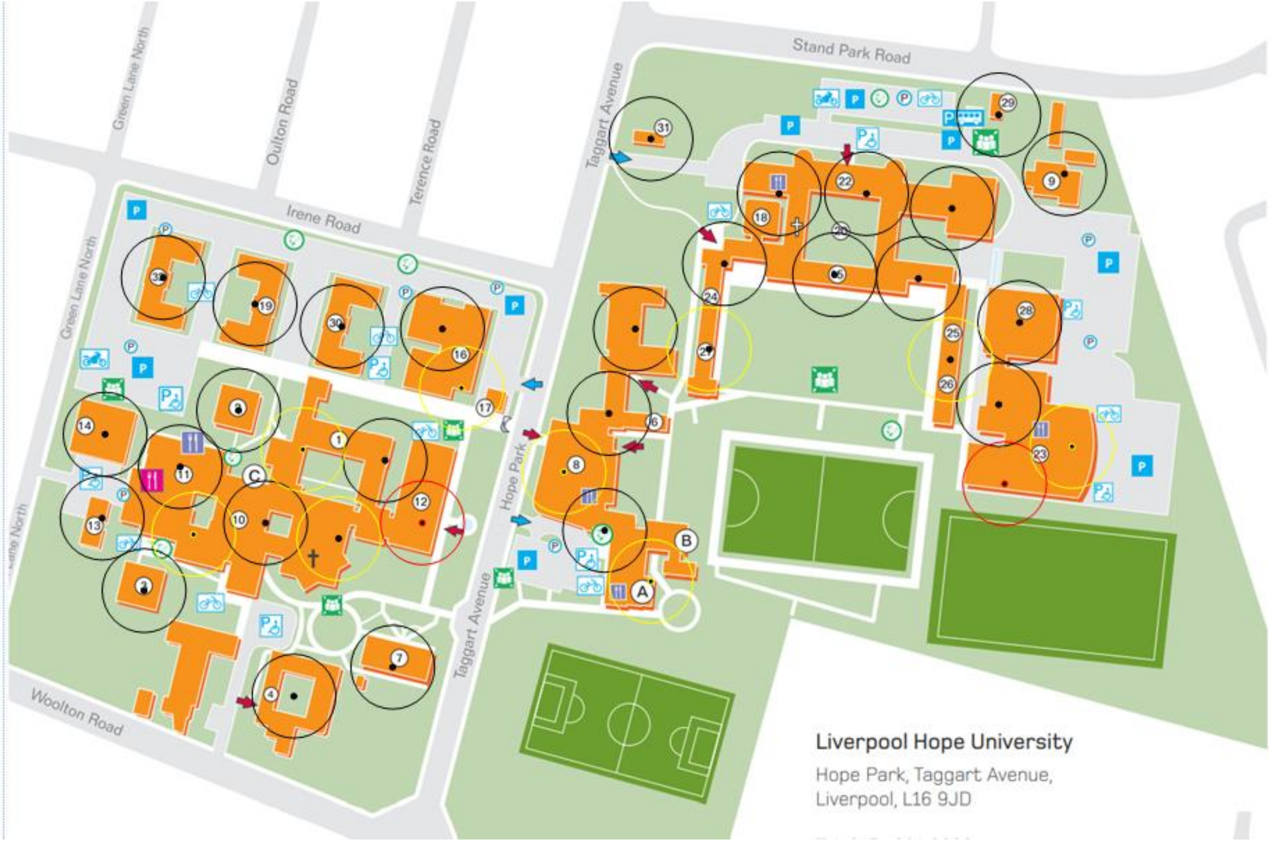
I am going to assume that the access points that we are using will be able to cover 40m well.

If a WAP can cover 40m well,
pi*r*r = pi*20*20 ≈ 1256m^2

Building #	Building Name	Length (m)	Width (m)	Area (m^2)	# of Floors (at highest)	Map reference number	# of Access Points Needed per building
1	Wesley Hall	50	25	1084	4	32	4
2	Newman Hall	50	25	1084	4	19	4
3	Teresa Hall	50	25	1084	4	30	4
4	Lecture Theatre Complex	50	35	1600	1	16	2
5	Green Lane Building	25	25	650	2	14	2
6	Angela Hall	20	20	455	3	2	3
7	Green Lane Annexe	22	10	230	2	13	5
8	Austin Hall	20	20	439	4	3	4
9	Conference Center	33	15	525	1	7	1
10	Business School	33	35	1126	3	4	3
11	Main Lodge	10	10	100	1	17	1
12	Gateway Building	50	15	900	3	12	3
13	Alexander Jones Building	50	25	1250	2	1	2
14	Frances Mary Lescher Building	50	15	750	4	10	4
15	Fresh Hope Food Court	50	54	2700	1	11	2
16	Chapel (Hope Park)	40	28	1120	1	5(Cross)	1
17	Taggart Lodge	15	7.5	112.5	2	31	2
18	Stand Park Lodge	11	6	66	2	29	2
19	Estates	24	13	312	1	9	1
20	Health Science Building	44	42	1848	2	28	4
21	Hope Park Sports	58	52	3016	2	23	6
22	St Elphin Hall	8	32.5	260	3	25	3
23	St Etheldrelda Hall	8	32.5	260	3	26	3
24	St Agnes Hall	8	32.5	260	3	24	3

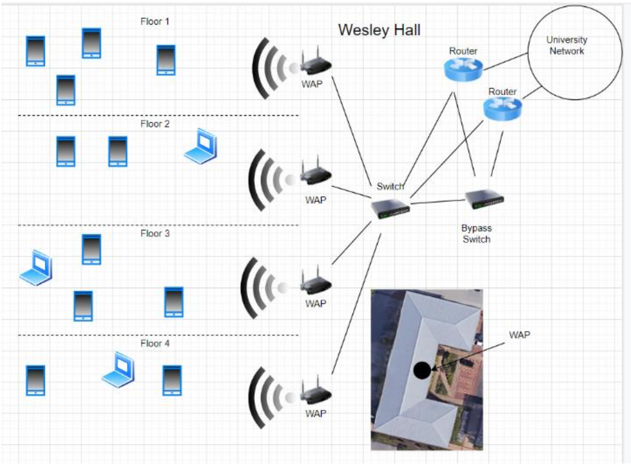
25	St Margaret Hall	8	32.5	260	3	27	3
26	The Markland	16	16	256	2	18	2
27	Hilda Constance Allen Building	55	12	660	3	15	3
28	Senate Room	38	10	380	1	21(Cross)	1
29	Quad	26	26	676	1	20	1
30	Sheppard Warlock Library	30	15	450	2	22	2
31	EDEN Building	60	35	2100	2	8	4
32	Chaplainncy	23	10	230	2	6	2
33	EDEN Lounge/Arbour Room	26	23	598	2	A	2
34	EDEN Suite	25	11	275	2	B	2

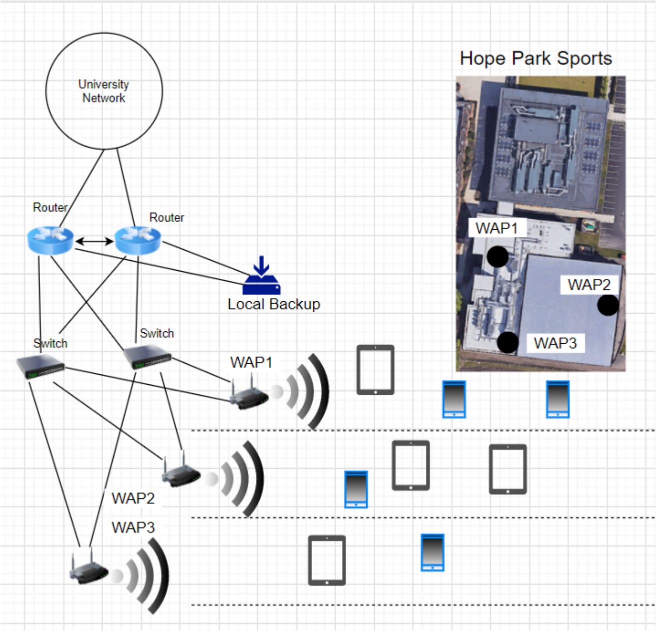
Part 2

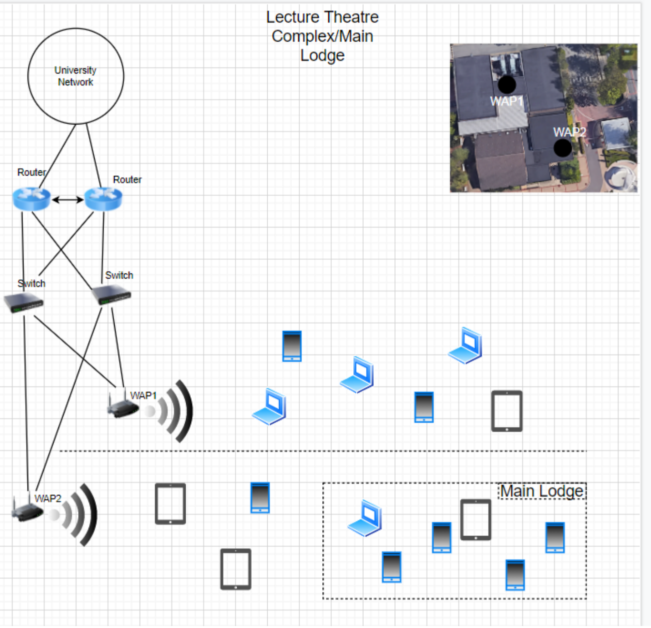


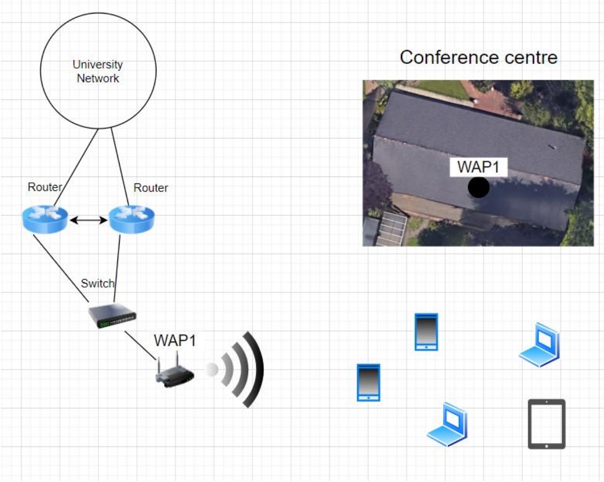
For part 2 my map is below that shows my recommended locations for the access points. This is very similar to my table in part 1 of the ICA but there are some small changes. For example, building 17 referenced on the map can share the network of the WAP I have placed in building 16. This would mean there it would be a waste of resources and money to place an access point each of the separate buildings. Another thing that I realized is that for building 23, 2 WAP covered most of the area of the building so I did not need 3 like the table above suggested. The different colors on the map represent the different channels on the network. I have managed to only require 3 channels in the entire network with minimal overlap.

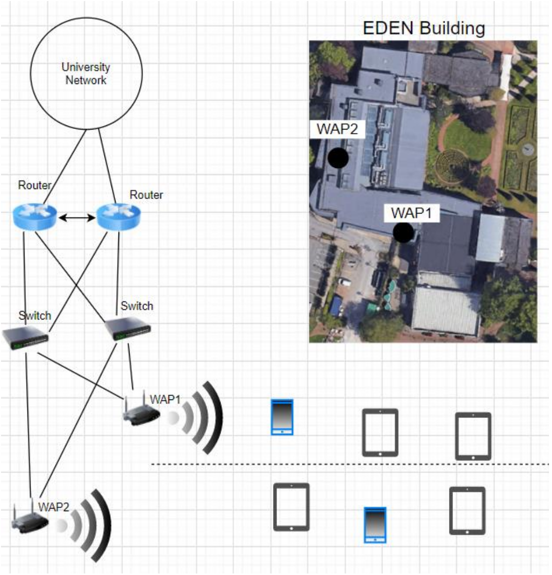
Part 3


Wesley Hall
Floor 1
Floor 2
Floor 3
Floor 4
WAP
WAP
WAP
WAP
WAP
Router
Router
University Network
Switch
Bypass Switch


Hope Park Sports
University Network
Router
Router
Local Backup
Switch
Switch
WAP1
WAP2
WAP3
WAP1
WAP2
WAP3


Lecture Theatre Complex/Main Lodge
University Network
Router
Router
Switch
Switch
WAP1
WAP2
WAP1
WAP2
Main Lodge


Conference centre
University Network
Router
Router
Switch
WAP1
WAP1


EDEN Building
University Network
Router
Router
Switch
Switch
WAP1
WAP2
WAP2
WAP1

Part 4

As with any wireless network, there are some inevitable security issues. The risk of an attack on the network is getting more and more prominent as wireless networks become larger and more complicated. I will cover some of the most common attacks on wireless networks and discuss some technologies used to attempt to best protect wireless networks.

War driving is a very common attack that is used to specifically target wireless networks. Otherwise known as parking lot attacks, "War-driving consists of a person in a moving vehicle searching for a wireless network using a laptop or a PDA." (Said et al,2012). The purpose of this attack is to gain access to a 'secure' wireless network to gain information that is stored there. Once inside the network, all devices that are using the network can be accessed, and often the attackers will use this blackmail or do other illegal activity on their devices.

(Said et al,2012) explains a fantastic example of when the American company TJX had one of its stores fall victim to war driving, when the criminal entered the network and downloaded millions of shopper's credit card information. This example shows how devastating an attack like this can be on a business and shows why care needs to be taken when protecting a network.

Spoofing is another very common attack used commonly on wireless networks. This is because it is one of the cheapest and easiest attacks to set up and run. Spoofing prays on unsuspecting people to defraud them of information by impersonating a trusted source online. This is very dangerous through wireless networks because there is no face to face contact with the devices. Someone might spoof an IP address to "bypass basic security measures such as firewalls that rely on blacklisting. This means that even if the attacker's original IP is on the blacklist and should be blocked, it will get through as they'll be hiding behind a spoofed IP." (NordVPN. 2019). Even some security measures like WPA could possibly not be able to stop spoofing and could be accessed by hackers by breaking down the access firmware and intercepting packets of information sent by routers in a network.

To help prevent against any spoofing attacks, you need to set up a wireless network properly. Because any wireless network is vulnerable, you need to make sure that you are using WPA2 protocols. This will make the network more robust and help prevent spoofing IP addresses within the network. Using more encryption like HTTPS will also help transfer information over wireless networks while inside the network.

WPA is an access protocol is old technology and many vulnerabilities have been found, which is why any safe network uses WPA2. This is a newer, safer version of WPA and helps to encrypt data quickly while keeping you safer from hackers.

One of the main reasons that WPA2 is so much safer than WPA is the encryption methods that is used. CCMP is a new standard of encrypting wireless networks that is used in WPA2. It has features that authenticates devices on the network, with proof of identity. It has much more power to restrict access than TKIP (used in WPA), as the layer management contributes to making a network more secure. TKIP was created for WPA and was a superior design to WEP protocols. As a standard, all networks should use WPA2 as it includes CCMP

An evil twin, or fake WAP attack is exactly what it sounds like. A hacker will set up a fake access point that poses as part for the network, waiting for the victims to connect to the network thinking that it is safe. Once that there are devices connected to this network, everything that they do can be tracked and recorded by the evil twin; meaning that if someone enters bank details while o the network, it is possible for the hacker to gain bank details of this person. This is obviously very dangerous but there are some common solutions to this type of attack.

Firstly, you should never connect to a network that you are not 100% certain is safe and secure. In addition to this, making sure that you do not enter sensitive information into any app or website while being connected to a public Wi-Fi is crucial to staying safe. A VPN can also be very helpful while connecting to untrusted networks.

A VPN works by connecting to a VPN server though your phone, before entering any online space. Doing so allows the vpn service to encrypt your information and acts as an untraceable block between any potential harm through the network ad your device, keeping it safe.

Part 5

Disaster policy:

I am going to assume that the university already has equipment to fulfil most of this disaster policy and will assume that we would be allowed to use these features of the university network that is already in place. It would be a good idea to backup information from the routers and switches into a store using a full backup every couple of weeks. This would help to restore procedures and information back to the devices if anything went wrong. If something occurred where a restore will need to happen it should be possible to get the latest backup and restore the switches and routers from a backup server. This procure should make the system much more available as any downtime caused by loss of data could be fixed quickly using the backup system.

There are some legal implications when installing a LAN that need to be planned in order to keep the university and individuals safe from prosecution. First, software licenses need to be dealt with properly, which includes making sure that each device that has access to software through the WLAN has permission from the software company, and they are aware of how the software is being distributed across the university networks. GDPR also needs to be considered within any service that collects data now, and a LAN is no different. Device information will be stored on the network and we need to make sure that the data being saved is being saved and protected safely. General GDPR guidelines are very common now and I will assume that other parts of the university will have their own procedure for this subject.

Part 6

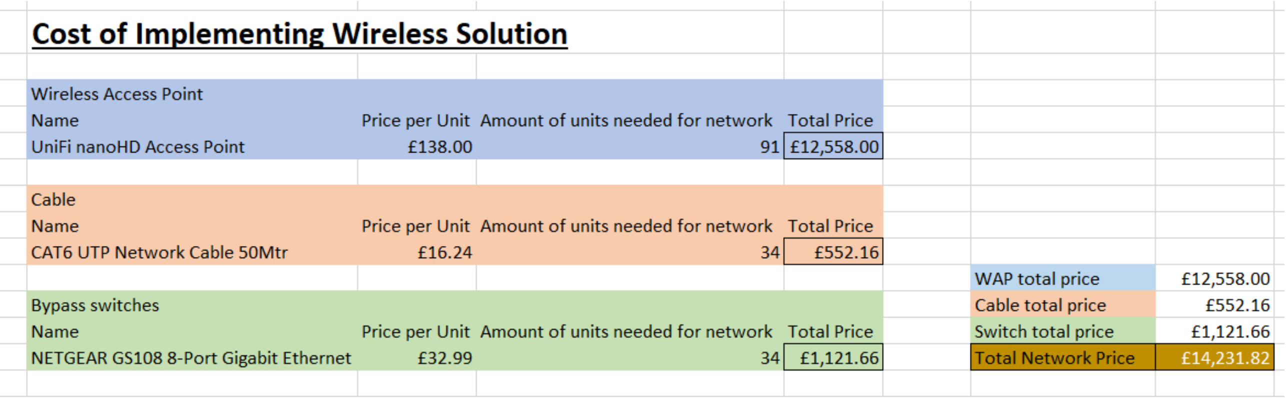
Because I will be planning on implementing a wireless network into already exiting buildings in an already existing university, I am going to assume that there are other technologies already in place in all of the buildings, it the university is in a high economy location. Therefore, I am going to assume that every building already has the appropriate routers and switches in order to run wired connections.

Something that I will not assume is that every building has bypass switches, as this is part of the security and backup policy and not essential to making the system work, so I will account for buying these along with the wireless access points for every building.

I will be calculating the cost of materials needed by researching some popular online retailers.

Retailer	Item Name	Price (£)	Link
TLC electrical supplies	CAT6 UTP Network Cable 50Mtr	16.24 (per 50m)	https://www.tlc-direct.co.uk/Products/CACAT6slash50.html
Unifi	UniFi HD Access Point	268	https://store.ui.com/collections/unifi-network-access-points
Unifi	UniFi nanoHD Access Point	138	https://store.ui.com/collections/unifi-network-access-points
Amazon	NETGEAR GS108 8-Port Gigabit Ethernet Network Switch	32.99	https://www.amazon.co.uk/NETGEAR-GS108UK-Gigabit-Ethernet-Unmanaged/dp/B0000E5SES/ref=sr_1_2?a=b&ascsubtag=trd-gb-5869882241983653000-21&dchild=1&keywords=Netgear+GS108&qid=1604512352&sr=8-2&tag=georiot-trd-21

In order to give an accurate network implementation cost, I am going to have to assume a couple of things about the system. I am going to give 50m of cable to every building that I am implementing a wireless access point into. I am also going to give 1 extra switch into each building to ensure that the university will have enough switches to fulfil the designs created.



Cost of Implementing Wireless Solution

Wireless Access Point

Name	Price per Unit	Amount of units needed for network	Total Price
UniFi nanoHD Access Point	£138.00	91	£12,558.00

Cable

Name	Price per Unit	Amount of units needed for network	Total Price
CAT6 UTP Network Cable 50Mtr	£16.24	34	£552.16

Bypass switches

Name	Price per Unit	Amount of units needed for network	Total Price
NETGEAR GS108 8-Port Gigabit Ethernet	£32.99	34	£1,121.66

WAP total price	£12,558.00
Cable total price	£552.16
Switch total price	£1,121.66
Total Network Price	£14,231.82

Bibliography:

H. Said, M. Guimaraes, N. Al Mutawa and I. Al Awadhi, "Forensics and war-driving on unsecured wireless network," 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, 2011, pp. 19-24.

NordVPN. 2019. What is IP spoofing and how can you protect yourself?. [ONLINE] Available at: https://nordvpn.com/blog/ip-spoofing/#:~:text=%20IP%20spoofing%20dangers%20%201%201%20Bypass,locations%20like%20cafes%20and%20airports.%20If...%20More%20. [Accessed 2 November 2020].