Network Infrastructure Report

James Duncan
Computer Systems, Infrastructure and Management

Contents

Problem Context

The Engineering and Computer Science department are getting an extension to their building and have given detailed floor plans. Both departments need access to their own independent network for their students however, both departments have shared spaces which need access to both sections of the network. A Theoretical network must be developed and plotted to suit the building's requirements whilst also making adjustments for the requirements of both departments.

This network will be designed theoretically using the 3 layer network design method to map how the network may be split up using VLANs, this will show how the network will be designed to allow for the shared area with full communication to other departments whilst keeping departments encapsulated in their own network. The deployed network must cater for the building restrictions therefore a network topology that suits the structure shall be recommended, these topologies state how the network connected devices in the distribution and access layers function in the network. These topologies include Bus, Star, Ring, Mesh, Tree and Hybrid. Each topology has its own advantages and disadvantages. Whatever topology is implemented the relevant physical devices must cater for redundancy to allow for a device to fail and the network to remain online. The network must cater for speed requirements of multiple computers accessing the network simultaneously without putting strain on the network from over allocations of network speed.

The building will have wireless connectivity which must be established alongside the development of the network. This will allow for students that bring their own devices (BYOD) or students that are not present at a computer but wish to access the network via mobile device. The network design must allow for further expansion in the future as it is possible that this building may go through further expansion due to the demand in industry for STEM (Science, Technology, Engineering, Maths.) graduates. As a result, this network shall be designed with future proofing in mind and where that is not possible an alternate method using the same equipment will be recommended.

Once a network design is established it will be theoretically deployed to find out the resources required to complete a full deployment into the building, from there it will be costed (using industry prices on reputable sites) including all the wiring required and any additional network items. This network must cater for all devices in the network for the Computer Science, Engineering and shared spaces, there are many Engineering and Computer Science spaces, to be connected but only 1 Pooled Computer Lab and several devices scattered along the hallways that require connections. There is also a Comms room which should act as the main entry point/egress layer to the network.

Many networking techniques will be deployed to ensure redundancy such as having multiple links with Spanning Tree Protocol (STP) to ensure packet efficiency and redundancy and VLAN network segmentation to establish a shared space. Security will be ensured by adding firewalls and other network-based solutions.

Solution

Three Layer Network Design

The network can be split up into three main segments, the core network which is the main processing for the whole environment. In this case this core network is likely to be part of the bigger university network. To ensure security from outside sources a firewall should be set up here before any connections enter or leave the network, this will block any connections that seem malicious to the network. The second layer (L3), Distribution (or Aggregation) connects all the interconnected switches together ensuring redundancy in the connections and laying the foundations for the connections made in the access layer. This layer is where the main network topologies will be laid out before each system is connected. Finally, the Access Layer (L2) connects all the systems to the distribution layer, including Computers, Mobile devices and Servers.

Splitting up the network using VLANs

As mentioned in the brief the two departments must be split up into separate networks, this can be achieved using VLANs (Virtual Local Area Networks). A VLAN splits connected devices up into groups where they can only talk to those in the same group, this can be achieved by having a L2 switch tag the ports where there is a connected device to a VLAN. For example, “Computer A” could be connected to “VLAN 2”, “Computer B” Could be connected to “VLAN 3”, “Computer C” to “VLAN 2”, both “A” and “C” can connect and communicate to each other but not “B”. In terms of the network traffic a switch can use VLAN Trunking to create a single virtual link that all VLAN data can travel across. It does this by tagging the header of each packet with a number that represents the origin/destination VLAN. Splitting up this network can be achieved by having 3 VLANs these include Computer Science, Engineering and Shared.

These VLANs are used to split up the devices into a separate network whilst residing in the same subnet, the Engineering and Computer Science VLANs contain all the devices for the relevant department although the shared contains both of these and the additional devices in the shared area. This can be done using a router set to inter-VLAN route between VLANs. An example of this could be when a computer in the Engineering VLAN wants to communicate with a computer on the shared VLAN, it would first check the switch for the connected computer, if it found nothing it would go to an L3 Router. This Router can then route the traffic to the relevant VLAN and find the device connected. The issue with this is that the Engineering and Computer Science VLANs would by default be able to communicate with each other which essentially means they are not separate networks, this can be fixed by enabling VLAN Access Control Lists (VACLs) (Cisco, 2018) on a switch to block or permit inter-VLAN Communications based on the IP address/Mac Address (Cisco, 2013). The default action for these VACLs is to block packets, however, these can be configured to do a series of other things including forwarding packets. This enables the shared VLAN to communicate with both Engineering and Computer Science, but Engineering and Computer Science cannot directly communicate with each other.

This method is fully expandable for all the other departments such as the Maths, Physics and Siemens network. Using these VLANs Isolates the network which achieves the requirement of separating the network but also allows for the shared spaces to have access to each department’s resources without exposing the rest of the network. However, it is worth noting that VLANs only exist on their relevant subnet, in this case the subnet could be global for the building. There could be more subnets that split up the departments, but those departments could not be part of the shared VLAN as they are not part of the same subnet. This can be deployed by using a L2 switch which supports VLANs, VACLs, and VLAN Trunking. Level 2 switches are then required to distribute the cables to the correct devices. However, this can also be deployed using level 3 switches that have functionality for VLANs, VLAN Access control lists and Routing, although it is worth checking if these switches support all the features required before purchasing them as most are just routers with additional features/ports. This method splits up network with the VLANs can be found in Appendix A (This is not a full deployment diagram it just demonstrates the VLANs data flow through the network and how VACLs permit and deny data).

The only issue with this setup is that there seems to be little reason why the shared VLAN requires access to all the devices of both Enginneering and Computer Science. This could actually be a security risk due to the access the shared VLAN gives to a user on a system over devices not in their department such as devices in the

thermofluids lab. This shared VLAN would make a lot more sense if Network Attached Storage (NAS) servers were deployed for each department and the shared VLAN had to acess both of them. As a result these severs could be isolated in their own VLANs and access given to the shared VLAN, in turn restricting device acess given to the shared VLAN whilst allowing it acess to the resources of both departments. The network structure can be found in appendix B and uses a very similar structure to the original deployment.

In summary in the above network you can see the egress point to the network with the mentioned firewall, this goes down into the main switches that would have multiple connections from the entry layer to ensure redundancy although not on this diagram for simplicity. This acts as the main routing point around the entire network. In the distribution section L3 Switches are assigned to allow for the shared network access using VLAN Access control. Finally, in the access layer all devices are connected via their department switches and routed to the switches in the distribution layer.

Building Network Topology

As mentioned in the problem context a network topology for the building must be recommended. In this case the building is so large that a hybrid approach must be deployed. Starting with the individual labs it makes sense to deploy a star network where each device is connected to a central hub/switch. If a singular device goes down then all the devices remain connected, the user could switch device to a system with an existing connection. Having a star topology in the rooms allows for controlling the bandwidth the rooms use allowing for restrictions to be put in place (Cisco, 2016) ensuring the network will not become overloaded and cause latency issues around the building. The main issue with this is that if the switch goes down then the entire room goes down, I suggest a small backup of switches is kept in order to replace a switch if it fails although care should be taken to ensure these stay up and running. However, due to the scalability of this topology it makes it perfect for the lab rooms as any device can just be added to the central switch. Other topologies would not work so well in these rooms as if something fails it could take the system down, additionally other topologies such as ring require you to take down the network and share bandwidth though the whole topology. This could create issues in large labs if everyone is sharing the same bandwidth.

For the small/medium office spaces these can all be connected using a tree topology where several rooms are connected to the same switch connected to the main line. This is because there are not many devices in these rooms that are required to be connected these switches can reside in the hallways and not necessarily in the rooms as this would take up quite a bit of space. This topology was chosen to allow for further connections in the small spaces and if one of the branches goes down it is possible to replace and manage the connection without too significant issue. As with the star topology if the core switch fails this can take down connectivity for all the offices connected. Star wasn't chosen for this as it takes a lot more resources to connect the same number of devices than it would take with tree and tree still has the same amount of flexibility for the offices. For large offices that have a lot of devices such as the technicians office it would be wise to implement a star methodology, but this should be done on a case by case basis.

Finally connecting all the rooms together can be achieved with a tree topology ensuring the network is all split up and there are limited key points of failure around the building that would cause the network to fail. Specifically, care should be taken to have multiple connections coming out of the Comms room to ensure connections stay up even if one of the switches goes down or a cable breaks. Using this topology also allows for segmentation of the building into multiple branches of the tree facilitating maintenance and network resilience. Other topologies were considered such as bus but that was not suitable for this network due to its half-duplex nature and its single point of failure for the entire network. Additionally, although the mesh topology would have allowed for a significant redundancy when connecting the labs, it would also make connections hard to manage especially as they tend to be both expensive and labour intensive.

In summary connections out of the Comms room are part of the building wide tree topology, lab rooms and large meeting rooms/ large office spaces are a star topology and finally the small/medium office spaces are connected via a tree topology. This can be seen in Appendix C.

Wireless

Wireless / Wi-Fi connectivity must be established in the building although there are many considerations that have to be established before deployment. Firstly, the Wireless devices should reside on the shared VLAN to allow for device access to both Computer Science and Engineering, although it would be possible to have separate access points in the network. The access points on the network should all be connected to a wireless controller in the Comms room that manages the access points and allows for further expansion(s) without configuring the settings of each access point. This also allows each access point to be on the same Service Set Identifier (SSID) which allows seamless communication between access points on the network. This means that a user can walk from one side of the building to another without wireless disruption. The wireless points themselves should be omni directional to give the widest range of coverage through the building although it is possible that the university could have set up a directional antenna outside of this building, but it is still worth ensuring the access points cover all areas of the building ensuring communication via Wi-Fi. The access points should also support dual band communications (Both 5GHz and 2.4GHz) for compatibility with all devices. Finally, user bandwidth and the amount of potential connections must be analysed before deployment to find out how many access points are required for the building.

Wireless access points can also make use of the Mesh Topology to propagate signals around each point which is especially useful if these access points have high levels of traffic (probable for the points in corridors or shared spaces) the network can find the fastest route to the Comms room therefore making the network faster. A mesh network can also survive a device breaking or dropping out and most importantly does not required a wired connection to each access point. As a result, few access points would need a full wired connection which saves money on the cabling required but will increase the amount of access points required. This network can be shown in Appendix D.

These Access Points can also make use of Power Over Ethernet (PoE) that provides power to the access point whilst connecting it to the network. Connecting these access points and enabling Mesh connectivity allows for significant redundancy if an access point drops. PoE requires a PoE compatible switch

Building Considerations

Certain aspects of the provided floorplan have a small cause for concern for a network deployment specifically the location of the Comms room. This room should be central to the building as it is where all the connections come from, as a result of its current location systems on the opposite side of the building may get inferior connections to the network than the side with the Comms room. The room also faces an exterior wall which could expose it to damp or flooding which could disrupt the network and damage equipment. Additionally, the Comms room is within range of mechanical equipment which can cause electronic interference specifically a series of mechanical risers next to the toilets. Finally, this Comms room is huge for this specific deployment although for future proofing could be useful. The siemens server room also falls short on some of these considerations as it is stationed close to two lifts.

There are several mechanical risers that can be used to wire the network between the floors, this should be taken into consideration when placing the equipment in the building for deployment. Several lifts are available to help deploy equipment to the building and there are several places where equipment can be stored in the building. These places include the electrical cupboard on the third floor, the general store rooms on the second floor and the Comms room itself.

Deployment

Throughput

The building has a total of 799 estimated devices (appendix E) in the Computer Science, Engineering and shared sections, each PC assuming maximum load would create a significant throughput of 799Gbits (1Gbit per machine) however, not all PCs require this specification as it is incredibly unlikely that they will use 1Gbit. 4K streaming requires 40Mbits which is significantly less than the 1Gbit, adjusting for loss of data each PC could be provided 100Mbits per machine 10% of the 1Gbit maximum throughput, this puts the throughput to 70.5Gbits. This throughput can be handled at the access layer by a 1Gbit switch that can provide all the PCs the

required throughput, this can be connected to a switch on the distribution layer that provides a 10Gbit throughput so each access layer switch has 10Gbits available to use, this allows for expansion of the room, machines and devices that require high levels of throughput. These distribution layer switches can be connected to the router which can serve 40Gbits of throughput. In turn this solution allows for each PC to have a 100Mb or higher connection and gives the availability to expand into other departments and labs.

Switches

There are many switches that can be chosen for this deployment however it is important to consider the throughput of the building, all PCs must be capable of 1Gbit speeds although they most likely will not need to use all that speed. Therefore, switches to serve the devices in the rooms are required this will take the uplink and share 1Gbit speeds to the devices connected. The second switch that is required will have to supply these switches with enough throughput to share around the devices, for this reason a switch with 40Gbit uplink and 10Gbit throughput should be able to serve these switches, although it will only serve 10Gbit to the switch the likelihood that a lab/office has 10 devices that are all using 1Gbit is very low and if that happens to be the case an additional switch with a different 10Gbit uplink can be added to support that demand.

Throughput is not the only demand for these switches as some of them will have to be Power Over Ethernet capable in order to provide the power to the access points, the switches will also have to support VLANs, VLAN Tagging, Spanning Tree Protocol and ACLs to provide the segmentation of the network and redundancy. There are a lot of companies that sell switches for enterprise however, most well-known are brands such as Cisco and Unifi as they have an ecosystem to their products that helps the network merge together and often come with very detailed instructions and warranty and support for their devices. Cisco, however, is incredibly expensive so as a result Unifi provision was looked into. Unifi seem to offer some of the best future proofing and visualisation for the network with their in-built app that helps you manage and operate the network with use of Augmented Reality (AR) technology, however, they fall with their warranty which only lasts 1 year from the date of shipment (Unifi, 2020). This may not be a problem if the devices are cared for and used correctly. The initial plan for this was to go purely with Unifi sourcing but they do not offer a switch with VACLs that have a high enough throughput to deliver 10Gbit through the network so this aspect would have to be sourced from other companies to deliver this throughput to the 1Gbit Unifi switches.

The chosen switches for this network are the S5850-48S6Q from FS which has a 5-year warranty and is capable of driving 10Gbit around the building. This Switch has Level 3 capabilities meaning it can route traffic around the network like a router it also has all the required features specified in the documentation (FS, 2020) like VLANs, VACLs and Trunking. The 1Gbit switch is the Unifi PoE+ 48 (500W) Switch which supports VLANS and spanning tree protocol according to its documentation (Unifi, 2020). This switch also supports PoE+ which can be used by the Access points.

Access Points & Controller

As mentioned above the use of the Unifi Ecosystem helps manage and control the network, as a result Unifi have created a tool (Unifi, 2020) where a user can set up and manage the access points in the network meaning the requirement for a controller is less important as you can manage all of the access points from this software. It can be hosted on a PC or on Unifi's own "cloud key" however any way it's hosted allows for the management of the Access points on the network. This software is eminently suitable for WIFI deployment as the software accurately shows you how effective your access points are being in your building allowing for fine tuning the deployment.

The chosen Access point for this deployment is the Unifi HD Access point which supports PoE and comes with pre included transformers if the switches output at a higher current than the access point can take. According to the specification (Unifi, 2020) it's dual band and supports VLANs it also is compatible with the software controller that Unifi provides allowing for management of the Access points. Other systems were considered but Unifi's software controller system is perfect for deployment especially as we already have a Unifi switch in the deployment.

In terms of throughput this switch can handle 1733Mbps on the 5Ghz band and 800Mbps on the 2.4ghz band leading to a full throughput of 2533 (Roughly 2.53Gbits) which is more than enough to serve all of the clients

on the network, its own documentation even states that it supports 100 Users at 300Mbps. Supplying this throughput to the Access point is simple as the access point itself has 2 Ethernet ports and will be connected to the other access points via the mesh network topology.

Router

The core router is one of the most expensive pieces of equipment required for this deployment due to the throughput requirements, this router is required to provide 40Gbit throughput in order to serve the switches in the distribution layer. This router also has to do all the routing and manage the firewall for the network. As a result of Unifi not having significant support for 40Gbit connections this router had to be sourced from a different company, unfortunately a significant amount of these routers require a quote from the company itself so prices range widely for these routers.

For this deployment the Juniper MX204 (Juniper, 2020) has been selected as it has up to 4 40 Gbit ethernet ports that can be used to drive the distribution layer, it has a maximum throughput of 400Gbits which is more than enough for the current building layout that has about 700 devices, This device can be deployed as it is impossible that the capacity would be exceeded even under heavy load. This leads to perfect future proofing where other departments can be connected up to it and still have throughput to spare if the building was to be further extended.

The next closest router in this line up is the MX240 (Juniper, 2020) which has 30 40Gbit ports and has a maximum throughput of 3.6TBs. Although this router would work it would be overkill for our network as the amount of throughput and ports provided would never be used in the medium term. It would be worth considering if the building was to have multiple servers, significantly more devices and more throughput requirements. The selected router could also be used to supply 10 Gbit to labs as it has ACLs that can be configured although these should be handled at the distribution layer. The issue with this router is that if it goes down the entire network fails as a result so extra care must be taken to ensure that this router is taken care of and even a possibility of a secondary router as a backup should be considered.

Wiring

For wiring of this network, the entry should be a fibre optic connection as this cable is more secure than a standard RJ45 Cat 6a cable, this can be used through the core layer as these cables are incredibly fast and reliable. Not much of this cable will be required as the rest of the network can use standard ethernet cables. The fibre cable chosen is Multi Mode OM3 as this cable can handle 40Gbit connections to the Comms room with little loss and it can handle data traffic being sent both ways along the fibre cable. To connect this cable to the router the correct transceiver will be needed, this can be purchase separately, in this case the Juniper QSFPP-40GBASE-SR4 transceiver can be bought with the requisite fibre cable to connect.

In terms of the rest of the building Cat 6a ethernet cable can handle 10Gbit connections so this will be used to transport and connect data out of the 10Gbit switch, however, it will also be used for the labs and offices as this allows for future proofing of the labs. Cat 5e could easily take the lab throughput however, if speeds in the building were upgraded and PCs required different speeds then the cables would need to be replaced hence why cat 6a should be used. Rolls of suitable quality ethernet cable can be bought online however, it is worth noting that in order to connect to devices a series of RJ45 connectors have to be bought and spliced into the cable. Additionally, if the cable has to go past any heavy machinery it would be worth buying shielded cable to ensure no disruption of the network or loss of packets.

The chosen Level 3 Switches cannot by default plug in ethernet cables such as cat 6a as they have an SFP+ connection, these are required to be transformed to ethernet so transceivers must be obtained to meet the needs of the switch.

Other Products

Several other products are required for this deployment that are more about logistics than the network itself, these are items like Uninterruptible Power Supplies (UPS) that give the network admins time to reliably shut down the network without suffering data loss in the event of a power cut. These UPS devices are only really required on critical infrastructure such as servers but in our case it is essential for the core layer devices such

as the router to have a UPS connections as this is one of the most expensive pieces of equipment in the entire network, if servers were to be deployed it would also be worth investing in a UPS for them. There are two types of UPS that can be used, the first is standby that acts as a battery bank in case of an outage but the more expensive safer version is the power line interactive UPS that smooths out irregularities in the current to the device and provides a backup battery. For this implementation a Power line interactive UPS will be implemented and range in price, however, the chosen UPS (APC BX1400UI) has several great reviews on Amazon.co.uk and costs £179.99 and is line interactive. This UPS also meets the power requirements for the router, the router consumes 0.5Watts per gigabit and at maximum it will consume 40Watts which is within the power output of the UPS.

Another item worth thinking about is cabinets and racking to store switches and the router on. Most cabinets have a max capacity measured in Rack Units, the router and switches have a 1U height meaning it will only require a single unit in the cabinet. A bigger cabinet should be bought for the Comms room however smaller ones should be bought for the labs as they require far less space. The chosen cabinets for this are a 42U cabinet for the Comms room, although this is overkill for the needs of this network it accommodates for expansion into servers and additional switches. This is costly at £1659.60 however ensures future proofing of the network. For the labs and other areas of the building a 12RU wall mounted cabinet which costs a more reasonable £192. Finally, for directing cables along hallways it would be preferable to use cable trunking to ensure no trip hazards and to cable manage the building. This is relatively inexpensive and basic variants can be picked up at most DIY suppliers.

Device	**Price (Per Unit)**
FS S5850-48S6Q 10Gbit Switch (Level 3)	£3829.20
Unifi PoE+ 48 Port 1Gbit Switch (Level 2)	£671.40
USW-Pro-24-POE Gen2 (Level 2)	£673.02
Unifi HD Access Point	£284.44
Cat 6a Shielded (100M)	£63.98
Cat 6a (100M)	£94.99
Juniper MX204 Router (Level 3)	£19,678.80
RJ45 Connectors (50 pack)	£10.59
10Gtek 10Gb/s SFP+ RJ45 Copper Transceiver	£66.99
MTP To MTP OM3) Fibre Trunk Cable (5M)	£73.20
Juniper QSFPP-40GBASE-SR4 Transceiver	£42
APC BX1400UI uninterruptible power supply	£159.34
12RU 19" 4-Post Wall Mount Network Cabinet	£192
42RU GR800-Series Black Cabinet	£1659.60
Wickes Self-Adhesive Mini Trunking (1M)	£2.37
Wickes Mini Trunking Flat Angle (Pack of 2)	£1.32
Wickes Mini Trunking Flat Tee	£1.29

These prices are the current prices as of 14/05/2020 without any discounts, however it is likely that an enterprise would get bulk prices for these products and discounts for the products.

Logical Deployment

Now that the devices have been selected it is possible to complete a logical deployment of this network, similar to the three-layer diagram but more focused on network connections and redundancy. The diagram can be found in appendix H. The diagram starts at the router that is located in the core layer of the network (Comms Room), this then spans into four separate switches (that take the 40Gbit uplink from the router) and utilise spanning tree protocol to ensure redundancy in the network. If a switch went down then the traffic can be forwarded to the next switch to keep the network running. These connections then go into the distribution and access layer which connects all the relevant devices. The second floor has more devices than the third floor as it has more labs, this means that the majority of connections on the second floor are in a star network. The offices were carefully connected to a tree network ensuring extra ports ready for expansion but also

bearing in mind the location of the rooms around the building as it would not be worth connecting the offices on the same switch from all the way across the building.

In terms of throughput although the network is likely to have less throughput per machine in the real world it can be calculated by how many PCs are connected to the 40Gbit uplink switches. For The second floor the 40 Gbit uplink shared amongst 491 devices will give the expected throughput of 81.46Mbits per user under max load which is more than sufficient, although at this point it is unknown how many access points may be connected so this will go down. On the Third floor the connected device numbers are far lower providing access to 308 devices and under full load could handle 130Mbits per user.

The main 4 switches configured with Spanning tree protocol can also be configured to have VACLs which stops inter VLAN Communications as per the three-layer diagram in appendix A, this layout also supports the layout with servers in appendix B allowing for future expansion. Although this diagram gives an accurate number of switches that will be required to connect to the network it misses a lot of additional products on the device list above, for this reason a physical deployment is required to understand how much cabling and other devices are required.

Physical Deployment

Now that the logical deployment of the building has been established and all the switches are deployed it is possible to start laying down the devices required in the building. Starting with the Comms room it requires all 4 of the main level 3 switches as this is where the main core of the network is. These should all be connected via OM3 Fibre optic to ensure fast speeds and a more secure line, these can then be stored in our 42RU cabinet that is bought for the server room, and the UPS plugged in to create our Comms room provision . Switches can then be placed in our 12RU mounted cabinets in the appropriate rooms and using cat 6a cable their appropriate star networks connected. These cabinets could be all centralised which would increase the amount of cabling but also decrease the amount of cabinets required. However, for this deployment the cabinets are deployed in each room. Once the devices in all the rooms are connected the core wiring must be laid down, this should make use of the risers where appropriate and holes drilled in the false ceiling where the cable can come down into the labs. According to the floor plans the longest cable required for this is 78 – 85M approximately, this is perfectly within the reach of the Cat6a specification which can handle up to 100M.

These cables should be Shielded as they travel directly next to or close to building plant such as the lifts that could cause electromagnetic interference. Once all the cabling is laid for the labs and switches it is time to consider access points, each lab should have an access point as this will alleviate pressure on the hallways and the labs Wifi connectivity this is especially relevant if the lab is being used for downloading as students may utilise their personal devices when downloading a big file (for example Arch Linux). Using a rule of thumb of having an access point every 150 square feet and judging by the access points maximum range there are a total of 51 access points connected to four switches in the network, this brings the throughput of the network down to about 94Mbits per second which achieves the goal of having at least 40Mbits per user and allows for a significant expansion as this network will be faster as that number assumes max load. These access points are all connected via 2 Ethernet cables and through the mesh network they create.

In terms of physical product delivery all of the devices will fit in the existing lifts so no product has to be lifted through the windows. Finally, once all wired trunking can be added to the deployment covering any protruding cables. The full deployment floor plans are detailed in appendix I and J however, they are difficult to read so supplied in appendix K there is a google drive link to the PDF versions of the floor plans.

This deployment is only theoretical so the number of devices connected should be the absolute minimum and several cable runs may not be possible as there may be reasons beyond existing knowledge that does not allow for drilling holes in certain walls (Electricity, Water etc). As a result, I suggest that these plans should be reviewed by an architect equipped with building plans and utility specialists, additionally precise measurements should be carried out to determine exactly how much cabling is required.

Cost Breakdown

As mentioned in the physical deployment a significant number of devices will be required to deploy this can be found in the table below but please note that these numbers could be subject to change, and it is just an estimate based on the floor plans in appendix I J and K. The actual cost of this may be in the range of £82,000 to £100,000 due to the knowledge of the building being limited. There may also be a demand for additional devices kept as spares such as the router or more / higher capability UPS devices to keep online different systems, there may also be a demand to connect the rest of the building to the network which could easily be handled by the amount of surplus capacity generated from the network so this would certainly increase the costs. Finally, there may be a demand for servers that could fit in the 42RU cabinet in the Comms room which would increase the price of deployment but also fit directly into the VLAN network as seen in appendix B.

Item	**Quantity**	**Total Cost**
Juniper MX204 Router (Level 3)	1	£19,678.80
Unifi PoE+ 48 Port 1Gbit Switch (Level 2)	26	£17,456.40
USW-Pro-24-POE Gen2 (Level 2)	11	£7403.22
FS S5850-48S6Q 10Gbit Switch (Level 3)	4	£15,216.80
Unifi HD Access Point	51	£14,506.44
RJ45 Connectors (50 pack)	34	£360.06
10Gtek 10Gb/s SFP+ RJ45 Copper Transceiver	37	£2,478.63
MTP To MTP (OM3) Fibre Trunk Cable (5M)	4	£292.8
Juniper QSFPP-40GBASE-SR4 Transceiver	8	£336
42RU GR800-Series Black Cabinet	1	£1659.60
Cat 6a Shielded (100M)	12	£767.76
Cat 6a (100M)	36	£3419.64
APC BX1400UI uninterruptible power supply	1	£159.34
12RU 19" 4-Post Wall Mount Network Cabinet	30	£5,952
Wickes Self-Adhesive Mini Trunking (1M)	221	£523.77
Wickes Mini Trunking Flat Angle (Pack of 2)	7	£9.27
Wickes Mini Trunking Flat Tee	1	£1.29
	Total	£82,817.31

As mentioned in the deployment section as a whole there was a desire to go with Unifi devices however this could lock us in their eco system specifically for the access points, Unifi's access points are all managed in their software which means if a third party access point was bought for our network it may have issues syncing up with the other access points, however due to the convenience and price of these access points it seems like a great system to go with. The rest of the network is not locked to any company as the entire core and distribution layers use separate vendors. There is a slight worry around warranty with all of the devices as unify only offer 1 year and others also only offer limited warranty. It may be beneficial to look into devices with greater warranties (or support contracts).

A considered written specification for installation should be produced, detailing the equipment, plans and deployment schedule (to minimise disruptions to current facility activity) and tender put out to multiple specialist contractors. As the installation costs are unknown these have not been included in this report but should be factored into the total costs.

Conclusion

In conclusion the selected network design will allow for all requirements laid down in the problem context, including throughput, WIFI connectivity, segmented network and Physical connectivity. This design has provision for for future proofing of the network by allowing more than enough throughput per device at maximum load, this allows the rest of the building to be connected to the network without hassle. VLANs have been carefully planned and edited to ensure security and upgradability with a server plan in mind when the departments want their own servers to host departmental resources. All known physical obstructions in the building have been carefully planned out and solution recommendations made.

Finally, a quick point about security. Most commercial entities handling significant data have a Security Operations Centre (SOC) this is where they manage and detect any foul play on the network. There are devices sold by companies like Unifi (the dream machine) which installs an Intruder protection system (IDS) onto the network, and other software such as Security Information and Event Management (SIEM) which allows a network admin to analyse in detail the traffic going in and out of the network. If the university does not have this facility I suggest it is considered in view of the vulnerabilities inherent in universities' data security.

Bibliography

Cisco. (2013, March 29). *Preventing Inter VLAN Routing*. Retrieved from Cisco Community : https://community.cisco.com/t5/switching/preventing-inter-vlan-routing/td-p/2151946

Cisco. (2016, May 02). *about "srr-queue bandwidth limit XX"*. Retrieved from Cisco Community: https://community.cisco.com/t5/switching/about-quot-srr-queue-bandwidth-limit-xx-quot/td-p/2793799

Cisco. (2018, May 6). *Chapter: Port ACLs (PACLs) and VLAN ACLs (VACLs)*. Retrieved from Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vacl.html

FS. (2020). *S5850 Series Switches*. Retrieved from FS: https://img-en.fs.com/file/datasheet/s5850-series-datasheet.pdf

Juniper. (2020). *MX Series 5G Universal Routing Platforms*. Retrieved from Juniper Network: https://www.juniper.net/uk/en/products-services/routing/mx-series/datasheets/1000597.page

Juniper. (2020). *MX204 Universal Routing Platform*. Retrieved from Juniper Networks: https://www.juniper.net/uk/en/products-services/routing/mx-series/mx204/

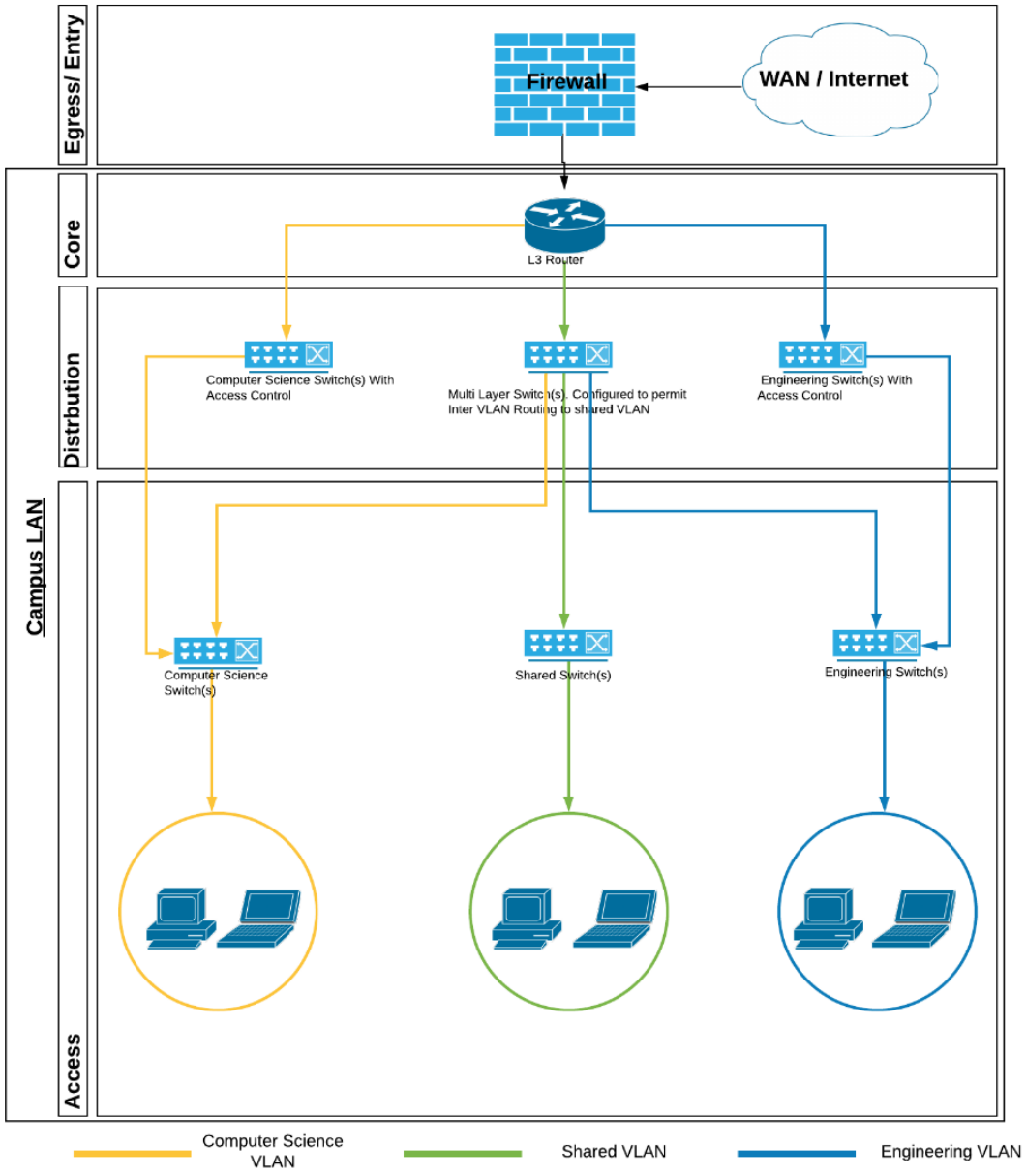
Unifi. (2020). *Network Management Controller*. Retrieved from unifi: https://www.ui.com/software/

Unifi. (2020). *Product Warranty*. Retrieved from Unifi : https://www.ui.com/support/warranty/

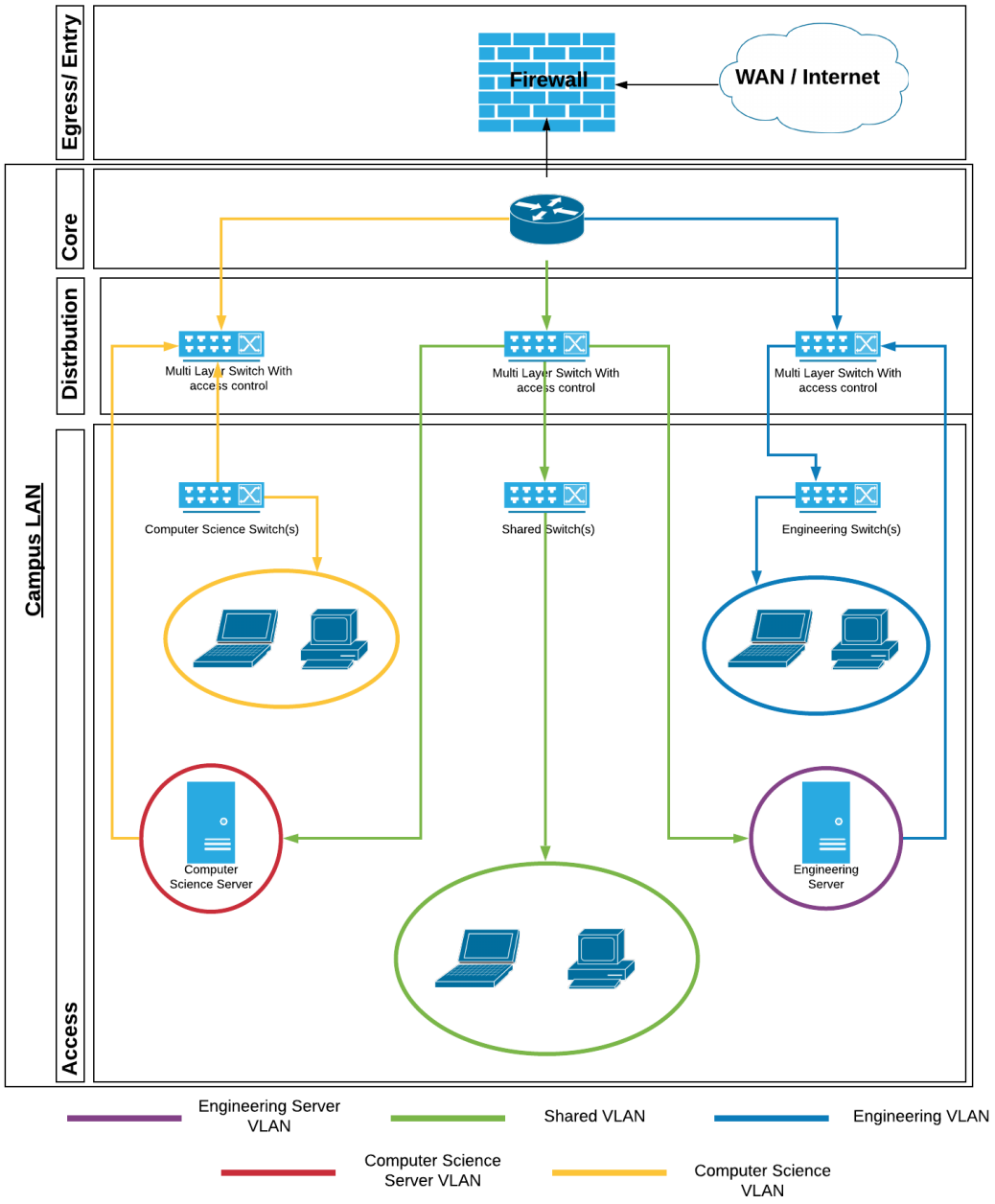
Unifi. (2020). *UAP-AC-HD*. Retrieved from Unifi: https://dl.ubnt.com/datasheets/unifi/UniFi_UAP-AC-HD_DS.pdf

Unifi. (2020). *Unifi Switch*. Retrieved from Unifi: https://dl.ubnt.com/datasheets/unifi/UniFi_PoE_Switch.pdf

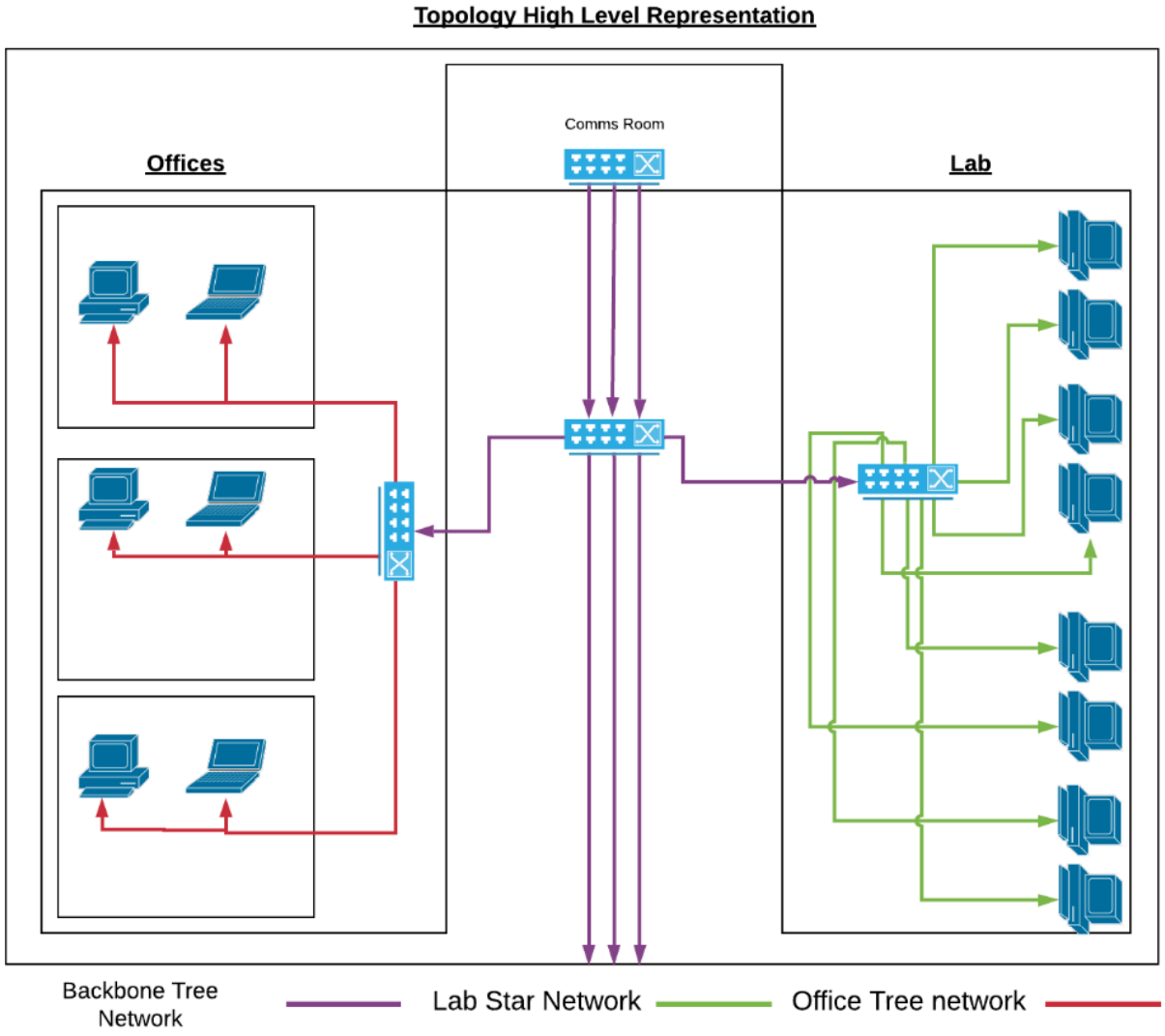
Appendix A – Layered Network Diagram



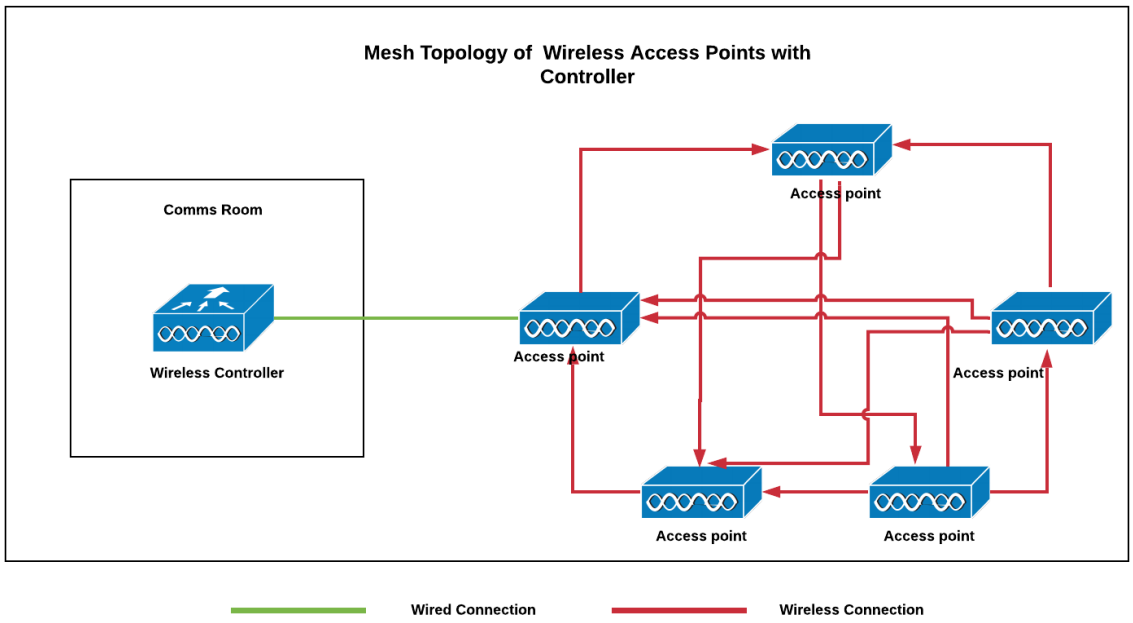
Appendix B – Layered Network Diagram (Using Server VLANs)



Appendix C – Physical Topology



Appendix D – Access Points Topology



Appendix E – Building PCs

Second Floor

Room	Number of rooms	Devices Per Room	Total Devices	VLAN
Computer Room	1	32	32	Engineering
Profs Office	10	2	20	Engineering
Dr Fuels Lab	1	20	20	Engineering
Project Lab 5	1	30	30	Engineering
Project Lab 4	1	24	24	Engineering
Project Lab 3	1	35	35	Engineering
Project Lab 2	1	25	25	Engineering
Project Lab 1	1	35	35	Engineering
Computer Lab 1	1	25	25	Engineering
ECR Office	1	6	6	Engineering
Materials Lab	1	25	25	Engineering
Single Office	7	2	14	Computer Science
Technical Support	1	2	2	Computer Science
Pooled Comp Lab	1	80	80	Shared
Computer Lab B	1	61	61	Computer Science
Computer Lab A	1	72	72	Computer Science
Computer Lab D	1	15	15	Computer Science
Computer Lab C	1	16	16	Computer Science
Research Staff	3	4	12	Computer Science
Copy Hub	1	2	2	Shared
Total	49	N/A	491	N /A

Third Floor

Room	Number of Rooms	Devices Per room	Total Devices	VLAN
Profs Office (Type 1)	4	3	12	Engineering
Profs Office (Type 2)	8	2	16	Engineering
Post Grad and RA	1	36	36	Engineering
HPL Hot Desks	1	4	4	Engineering
Communications Laboratory (CaDE)	1	18	18	Engineering
Technicians Office	1	4	4	Engineering
Office	11	2	22	Engineering
Computer Lab 2	1	15	15	Engineering
Single Office	20	2	40	Computer Science
Large Office w/Meeting	4	6	24	Computer Science
Research Student Workplaces	1	24	24	Computer Science
Bookable Breakout Area	1	24	24	Computer Science
Research Staff	1	4	4	Computer Science
Hourly Paid Lecturers	1	6	6	Computer Science
Unnamed Room	1	8	8	Computer Science
Research Student Workplaces	1	21	21	Computer Science
PA to HOS	1	2	2	Computer Science
HOS	1	6	6	Computer Science
Copy Hub	1	2	2	Shared

Linux Network Printer and storage	1	2	2	Shared
Project Lab 6	1	16	16	Engineering
Printer	2	1	2	Shared
Total	64	N/A	308	N/A

Appendix F – Links to chosen Devices

https://www.fs.com/uk/products/29123.html

https://store.ui.com/collections/unifi-network-routing-switching/products/unifiswitch-48-500w

https://eu.store.ui.com/products/usw-pro-24-poe-gen2

https://store.ui.com/collections/wireless/products/unifi-hd

https://www.amazon.co.uk/External-COPPER-Double-Network-Outdoor/dp/B01GK898I0/ref=psdc_430464031_t1_B01HVTV448

https://www.amazon.co.uk/CAT6A-Copper-Network-10GBASE-T-Ethernet-Lilac-Violet/dp/B00L46YWRG

https://www.amazon.co.uk/BeMatik-Ethernet-network-40GBase-T-category-Blue/dp/B07NYXB3YM

https://www.amazon.co.uk/10Gtek-Transceiver-Compatible-SFP-10G-T-S-UF-RJ45-10G/dp/B01M8O3MAL

https://www.it-market.com/en/juniper-mx204-ir1?gclid=CjwKCAjwqdn1BRBREiwAEbZcR5KVDaTVSgY8m4J7LfVTdsQdjJfRcfpKcj3iVGFHRS5197JRS8evthoCBpUQAvD_BwE

https://www.juniper.net/uk/en/products-services/routing/mx-series/mx204/

https://www.fs.com/uk/products/36439.html

https://www.fs.com/uk/products/68023.html

https://www.amazon.co.uk/APC-Back-UPS-BX-BX1400UI-Uninterruptible/dp/B00T7BYPDG/ref=sxbs_sxwds-stvp?cv_ct_cx=Power+line+interactive+UPS&dchild=1&keywords=Power+line+interactive+UPS&pd_rd_i=B00T7BYPDG&pd_rd_r=51d8c2e2-418a-4bdf-b5c3-8334c12e7433&pd_rd_w=IoSQf&pd_rd_wg=cGMqR&pf_rd_p=d9b87ec0-c7c2-464c-b8a6-2e7b5576127a&pf_rd_r=SREYDEMTPP9VMM9CH5ZC&psc=1&qid=1589117193&sr=1-1-718396de-69ac-46a0-9195-9669ab0086b2

https://www.fs.com/uk/products/75869.html

https://www.fs.com/uk/products/73579.html

https://www.wickes.co.uk/Wickes-Self-Adhesive-Mini-Trunking---White-16-x-25mm-x-2m/p/712947

https://www.wickes.co.uk/Wickes-Self-Adhesive-Mini-Trunking---White-16-x-25mm-x-2m/p/712947

https://www.wickes.co.uk/Wickes-Mini-Trunking-Flat-Angle---White-25-x-16mm-Pack-of-2/p/715029

https://www.wickes.co.uk/Wickes-Mini-Trunking-Flat-Tee---White-25-x-16mm/p/109678

Appendix G – Product spreadsheets

Switch	Uplink	PoE	Ports	Level	Company	Throughput	Price	VLAN	STP	ACLs	Link
S5850-48S6Q	40Gbit	NO	48	L3	FS	10Gbit	3829.2	YES	YES	YES	https://www.fs.com/uk/products/29123.html
UniFi Switch PoE+ 48 (500W)	10GBit	PoE+	48	L2	Unifi	1Gbit	671.4	YES	YES	NO	https://store.ui.com/collections/unifi-network-routing-switching/products/unifiswitch-48-500w
M4300-48X	40Gbit	PoE+	48	L3	Netgear	10Gbit	4772.49	YES	YES	YES	https://www.netgear.co.uk/business/products/switches/managed/M4300-48X.aspx#tab-techspecs
M4300-52G-PoE+ 550W PSU	10Gbit	PoE+	48	L2	Netgear	1Gbit	2064.24	YES	YES	YES	https://www.netgear.co.uk/business/products/switches/managed/M4300-52G-PoE-plus-550W-PSU.aspx#tab-techspecs
S3900-48T4S	10Gbt	NO	48	L2+	FS	1Gbit	462	YES	YES	YES	https://www.fs.com/uk/products/72946.html
S5500-48T8SP	1Gbit	PoE+	48	L3	FS	1Gbit	1478.4	YES	YES	YES	https://www.fs.com/uk/products/83325.html
S5850-48T4Q	40Gbit	NO	48	L3	FS	10 Gbit	4424.4	YES	YES	YES	https://www.fs.com/uk/products/69378.html

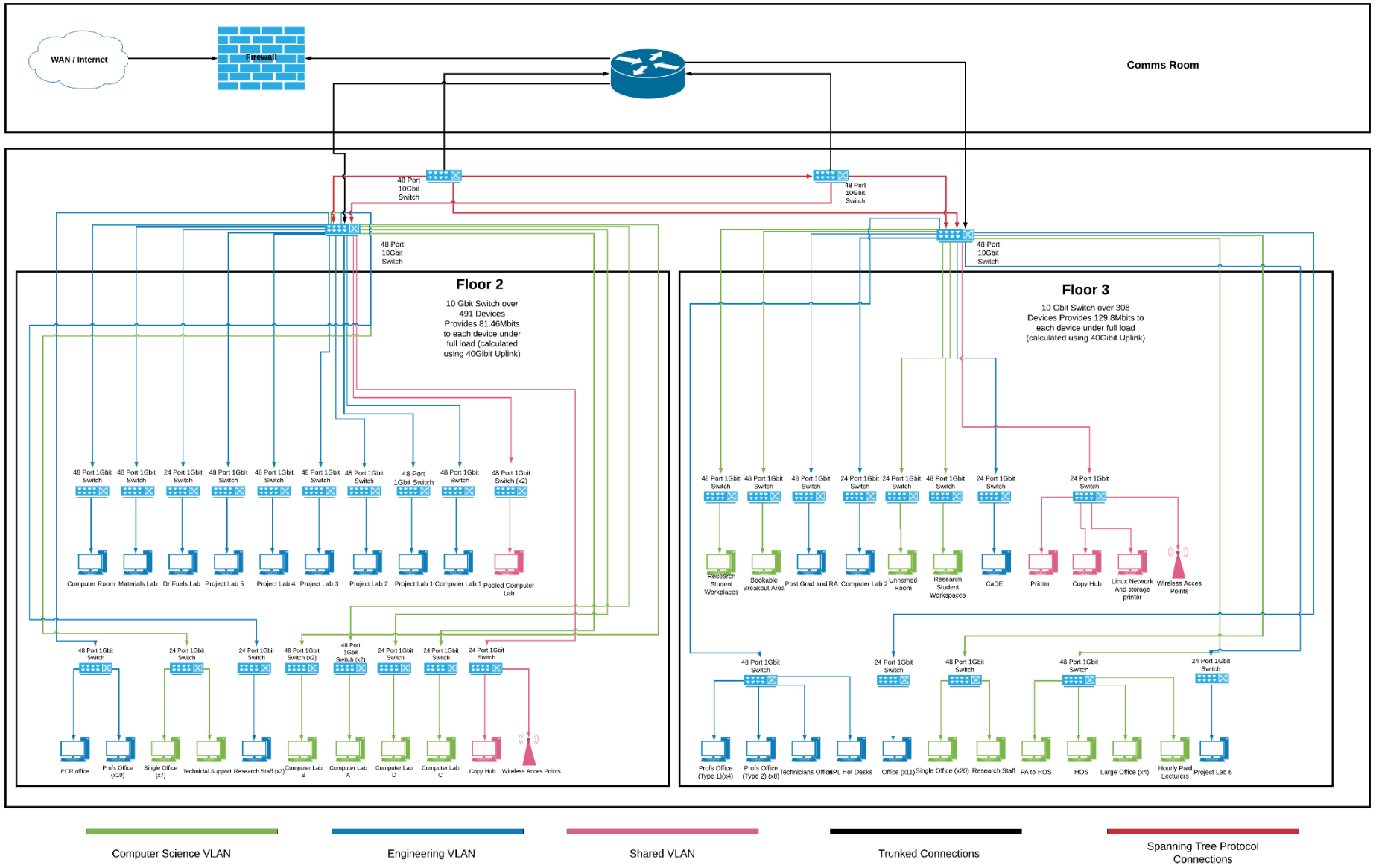
Cable	Type	Sheilde	Length	Amount	Link
Ethernet	Cat 6a	Yes	100 M	63.98	https://www.amazon.co.uk/External-COPPER-Double-Network-Outdoor/dp/B01GK898I0/ref=psdc_430464031_t1_B01HVTV448
Ethernet	Cat 6a	No	100M	94.99	https://www.amazon.co.uk/CAT6A-Copper-Network-10GBASE-T-Ethernet-Lilac-Violet/dp/B00L46YWRG
Ethernet	Cat 8	No	20M	46.99	https://www.amazon.co.uk/BeMatik-Ethernet-network-40GBase-T-category-Blue/dp/B07NYXB3YM

Router	40GBit	Firewall	Company	Price	Link
Juniper PTX1000	YES (30 Ports)	YES	Juniper	71736.22	https://www.insight.com/en_US/shop/product/PTX10001-20C-AO/JUNIPER%20NETWORKS/PTX10001-20C-AO/JuniperNetworksPTXSeriesPTX10001-20C-AO-Router-40GigabitLAN,100GigabitEthernet-rack-mountable/
""	""	""	""	""	https://www.juniper.net/uk/en/products-services/routing/ptx-series/ptx1000/
Juniper MX204	YES (4 Ports)	YES	""	£19,678.80	https://www.juniper.net/uk/en/products-services/routing/mx-series/mx204/

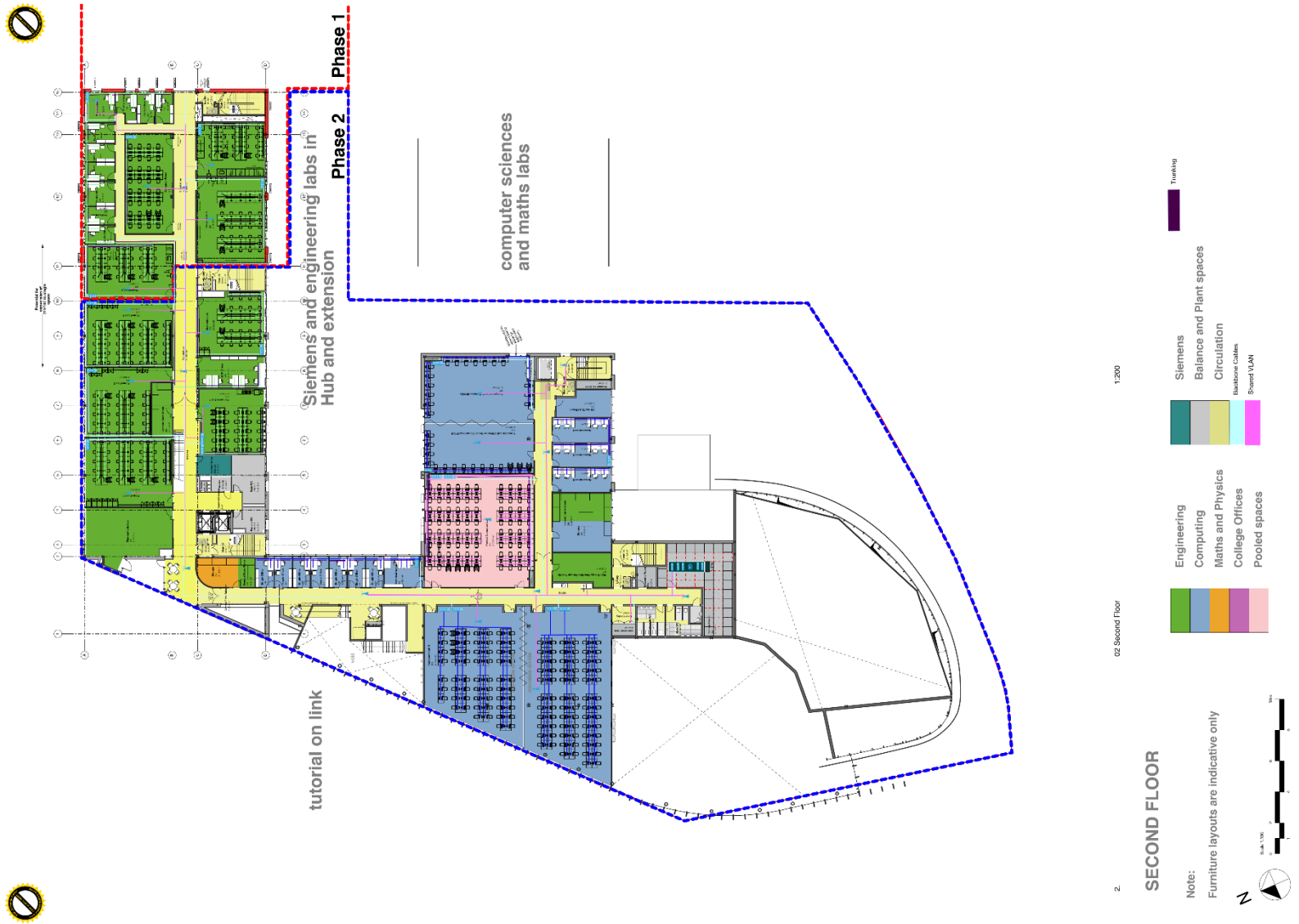
Access Points	Dual Band	Ports	PoE	VLAN	Company	Price	Link
UniFi HD Access Point	YES	2	802.3at (Transformer Pre included)	YES	Unifi	282.44	https://store.ui.com/collections/wireless/products/unifi-hd

Other	
12 Fibres MTP to MTP Female Plenum (OM3)	https://www.fs.com/uk/products/68023.html
50 Pack RJ45 Connectors 10	https://www.amazon.co.uk/VCE-50-Pack-Connector-Ethernet-Plug-50u-50-Pack-End-Pass-Through/dp/B07MM3FQ3F/ref=sr_1_3?crid=ZDDU829GH208&dchild=1&keywords=rj45+connector&qid=1588783714&s=electronics&sprefix=RJ4%2Celectronics%2C139&sr=1-3
42U Cabinet	https://www.fs.com/uk/products/73579.html
12U Cabinet	https://www.fs.com/uk/products/73869.html
Juniper Networks QSFPP-40GBASE-SR4 Compatible 40GBASE-SR4 QSFP+	https://www.fs.com/uk/products/76439.html
APC by Schneider Electric Back-UPS BX - BX1400UI	https://www.amazon.co.uk/APC-Back-UPS-BX-BX1400UI-Uninterruptible/dp/B00T7BYPDG/ref=sxbs_sxwds-stvp?cv_ct_cx=Power+line+interactive+UPS&dchild=1&keywords=Power+line+interactive+UPS&pd_rd_i=B00T7BYPDG&pd_rd_r=51d8c2e2-418a-4bdf-b5c5-8354c12e7433&pd_

Appendix H – Logical Deployment Diagram (Zooming into this diagram is required)


WAN / Internet
Firewall
Comms Room
48 Port 10Gbit Switch
48 Port 10Gbit Switch
48 Port 10Gbit Switch
48 Port 10Gbit Switch
Floor 2
10 Gbit Switch over 491 Devices Provides 81.46Mbits to each device under full load (calculated using 40Gibit Uplink)
48 Port 1Gbit Switch
48 Port 1Gbit Switch
24 Port 1Gbit Switch
48 Port 1Gbit Switch
48 Port 1Gbit Switch
48 Port 1Gbit Switch
48 Port 1Gbit Switch
48 Port 1Gbit Switch
48 Port 1Gbit Switch
48 Port 1Gbit Switch (x2)
Computer Room
Materials Lab
Dr Fuels Lab
Project Lab 5
Project Lab 4
Project Lab 3
Project Lab 2
Project Lab 1
Computer Lab 1
Pooled Computer Lab
48 Port 1Gbit Switch
24 Port 1Gbit Switch
24 Port 1Gbit Switch
48 Port 1Gbit Switch (x2)
48 Port 1Gbit Switch (x2)
24 Port 1Gbit Switch
24 Port 1Gbit Switch
24 Port 1Gbit Switch
ECR office
Profs Office (x10)
Single Office (x7)
Technicial Support
Research Staff (x3)
Computer Lab B
Computer Lab A
Computer Lab D
Computer Lab C
Copy Hub
Wireless Acces Points
Floor 3
10 Gbit Switch over 308 Devices Provides 129.8Mbits to each device under full load (calculated using 40Gibit Uplink)
48 Port 1Gbit Switch
48 Port 1Gbit Switch
48 Port 1Gbit Switch
24 Port 1Gbit Switch
24 Port 1Gbit Switch
48 Port 1Gbit Switch
24 Port 1Gbit Switch
24 Port 1Gbit Switch
Research Student Workplaces
Bookable Breakout Area
Post Grad and RA
Computer Lab 2
Unnamed Room
Research Student Workspaces
CaDE
Printer
Copy Hub
Linux Network And storage printer
Wireless Acces Points
48 Port 1Gbit Switch
24 Port 1Gbit Switch
48 Port 1Gbit Switch
48 Port 1Gbit Switch
24 Port 1Gbit Switch
Profs Office (Type 1)(x4)
Profs Office (Type 2) (x8)
Technicians Office
HPL Hot Desks
Office (x11)
Single Office (x20)
Research Staff
PA to HOS
HOS
Large Office (x4)
Hourly Paid Lecturers
Project Lab 6
Computer Science VLAN
Engineering VLAN
Shared VLAN
Trunked Connections
Spanning Tree Protocol Connections

Appendix I – Second Floor Plan



Appendix J – Third Floor Plan

3. 03 Third Floor 1:200

THIRD FLOOR

Note:

Furniture layouts are indicative only

N

Scale 1:100

Engineering
Computing
Maths and Physics
College Offices
Pooled spaces
Siemens
Balance and Plant spaces
Circulation
Backbone Cables
Shared VLAN

Appendix K – Google Drive Link

https://drive.google.com/drive/folders/1KOOgi81Ls36Sw_cGGlKw-2hPAcd8Dffd?usp=sharing