|  |  |
| --- | --- |
|  | Network Infrastructure Report |
|  |  |
|  | James Duncan  Computer Systems, Infrastructure and Management  [Date] |

**Contents**

[Problem Context 2](#_Toc39674081)

[Solution 3](#_Toc39674082)

[Three Layer Network Design 3](#_Toc39674083)

[Splitting up the network using VLANs 3](#_Toc39674084)

[Building Network Topology 5](#_Toc39674085)

[Wireless 6](#_Toc39674086)

[Building Considerations 7](#_Toc39674087)

[Deployment 8](#_Toc39674088)

[Switches 8](#_Toc39674089)

[Access Points & Controller 8](#_Toc39674090)

[Wiring 9](#_Toc39674091)

[Physical Deployment 9](#_Toc39674092)

[Logical Deployment 9](#_Toc39674093)

[Cost Breakdown 9](#_Toc39674094)

[Conclusion 9](#_Toc39674095)

[Bibliography 10](#_Toc39674096)

[Appendix 11](#_Toc39674097)

[Layered Network Diagram (Using Server VLANs) 11](#_Toc39674098)

# 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 buildings 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 the departments encapsulated in their own network. The deployed network must cater for the building therefore a network topology that suits the building 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 implemented, and 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 at once 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 phone. The network design must allow for further expansion in the future as it is possible that this building may go through another 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 how many resources are required to complete a full deployment to the building, from there it will be costed up (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 amongst all the Computer Science, Engineering and shared spaces, there are many Engineering spaces, 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 Scanning Tree Protocol (STP) so 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

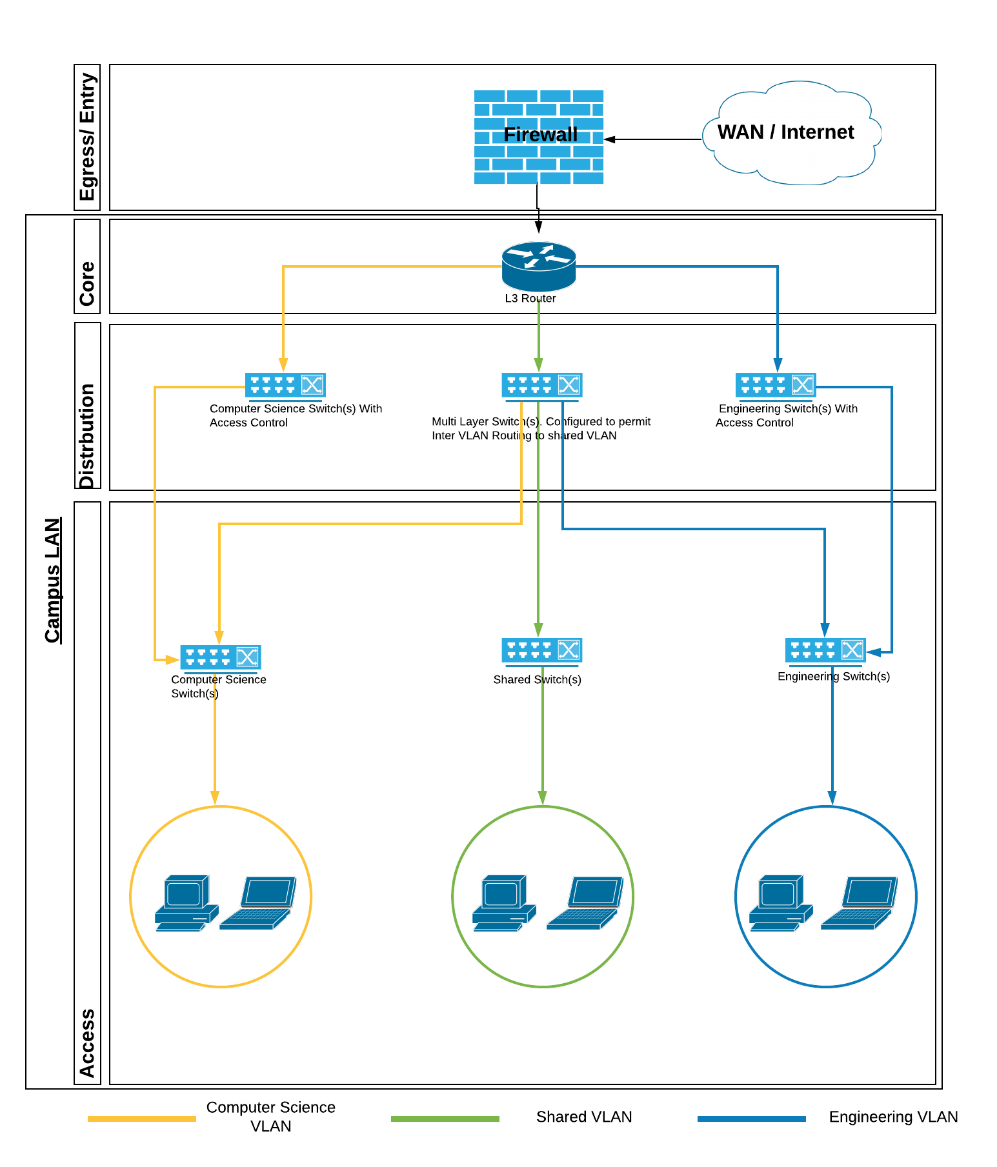
The network can be split up into three main segments, the core network which is the main processing for the whole environment. In this case this core network is likely to be part of the bigger network around the university. To ensure security from outside sources a firewall should be set up here before 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, Mobiles 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 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, this can be configured to do a series of other things including forwarding packets. This enables the shared to communicate with both Engineering and Computer Science, but Engineering and Computer Science cannot 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 departments 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 is 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 this switches support all the features required before buying them as most are just routers with additional features/ports. This method splits up network with the VLANs can be found in Figure 1 (This is not a full deployment diagram it just demonstrates the VLANs data flow through the network and how VACLs permit and deny data).



*Figure 1: Layered VLAN Network*

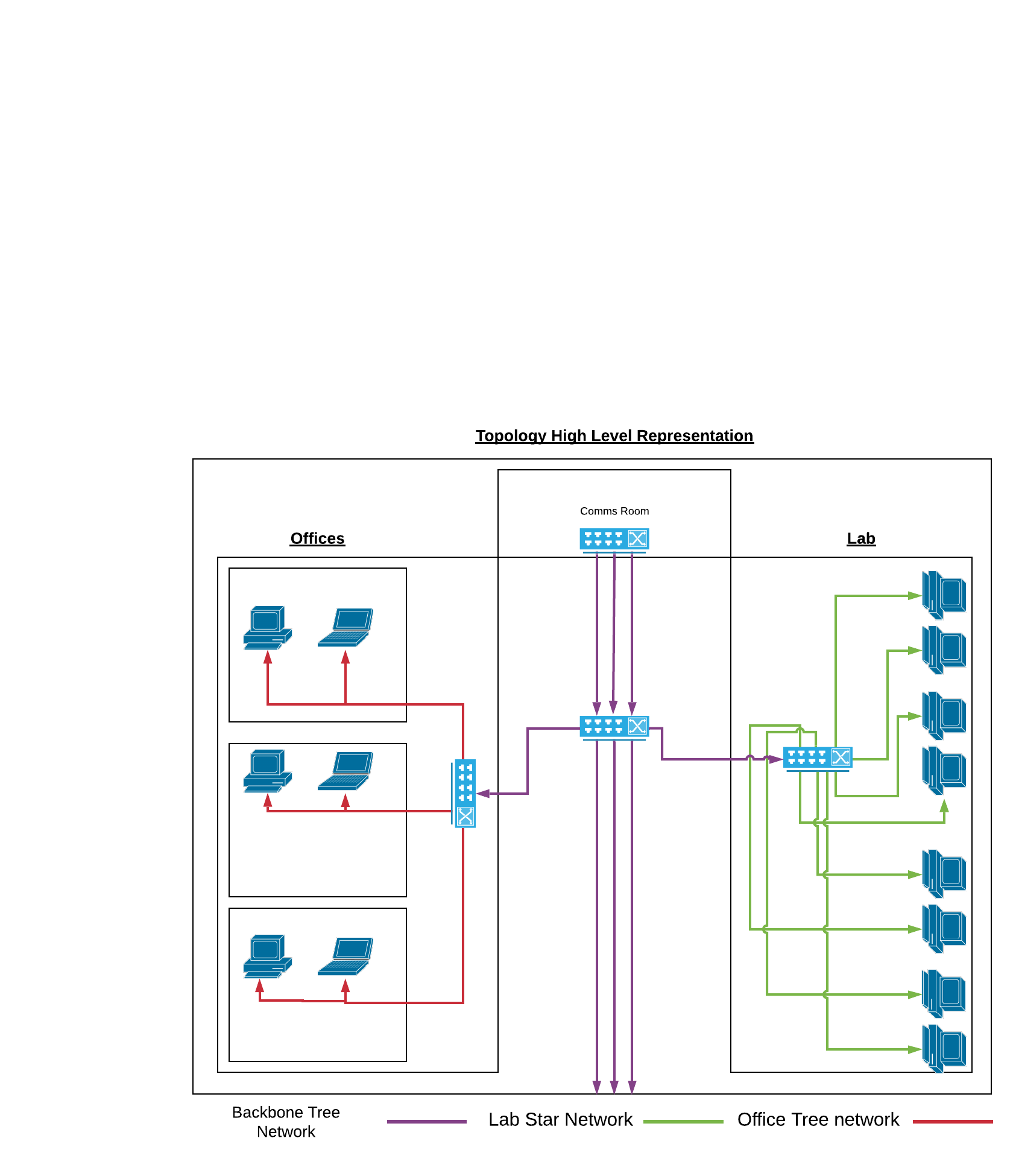
The only issue with this setup is that there seems to be little reason why shared VLAN requires access to all the devices on both Enginneering and Computer Science. This could actually be a security risk due to the freedom the shared VLAN gives to a user on a system over devices not in their department 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 the the shared VLAN whilst allowing it acess to the resources of both departments. The network structure can be found in the appendix 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 so if a singular device goes down then all the devices in the lab are still 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 overcrowded 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 does go down 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 as there are not many devices in these rooms that are required to be connected these switches an 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 space and if one of the branches goes down it is possible to replace and manage the connection without too much hassle. 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 to 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 go down. 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 resulting in easier 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 amount of redundancy when connecting the labs, it would also make connections hard to manage especially as they tend to be 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 figure 2.

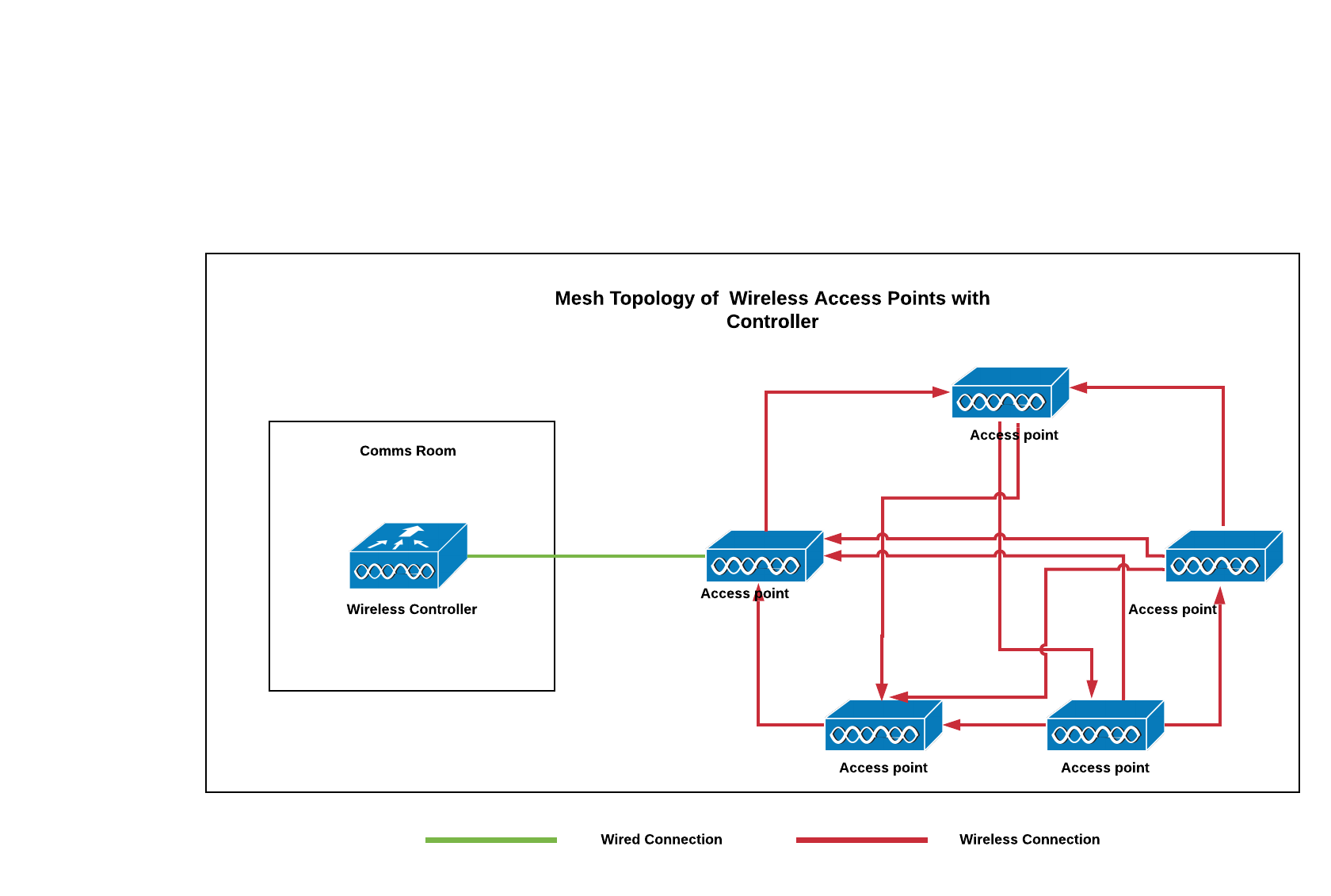


*Figure 2: Topology High Level Representation*

## Wireless

Wireless or 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 access to devices for 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 expansions without messing with 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 from access point to access point in 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 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 figure 3.



*Figure 3: Mesh Topology of Wireless Access Points with Controller*

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 worry 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 worse 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

## 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 the most likely will not need to use all that speed. Therefore, a switch 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, Scanning 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 like Cisco and Unifi as they have an ecosystem to their products that helps the network merge well together and often come with very detailed instructions and great warranty and support for their devices. Cisco, however, is incredibly expensive so as a result Unifi 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). Although this may not be a problem if the device is cared for and used correctly. The initial plan for this was to go purely with Unifi but they do not offer a switch with high enough throughput to deliver 10Gbit through the network so other companies would have to be outsourced 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 its hosted allows for the management of the Access points on the network. This software is incredible 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 that is being deployed.

## Wiring

## Physical Deployment

## Logical Deployment

## Cost Breakdown

# Conclusion

# 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

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

## Layered Network Diagram (Using Server VLANs)