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

**Contents**

[Problem Context 2](#_Toc39324997)

[Solution 3](#_Toc39324998)

[Three Layer Network Design 3](#_Toc39324999)

[Splitting up the network using VLANs 3](#_Toc39325000)

[Alternate Network Layouts 5](#_Toc39325001)

[Building Network Topology 5](#_Toc39325002)

[Wireless 6](#_Toc39325003)

[Building Considerations 6](#_Toc39325004)

[Conclusion 6](#_Toc39325005)

[Bibliography 7](#_Toc39325006)

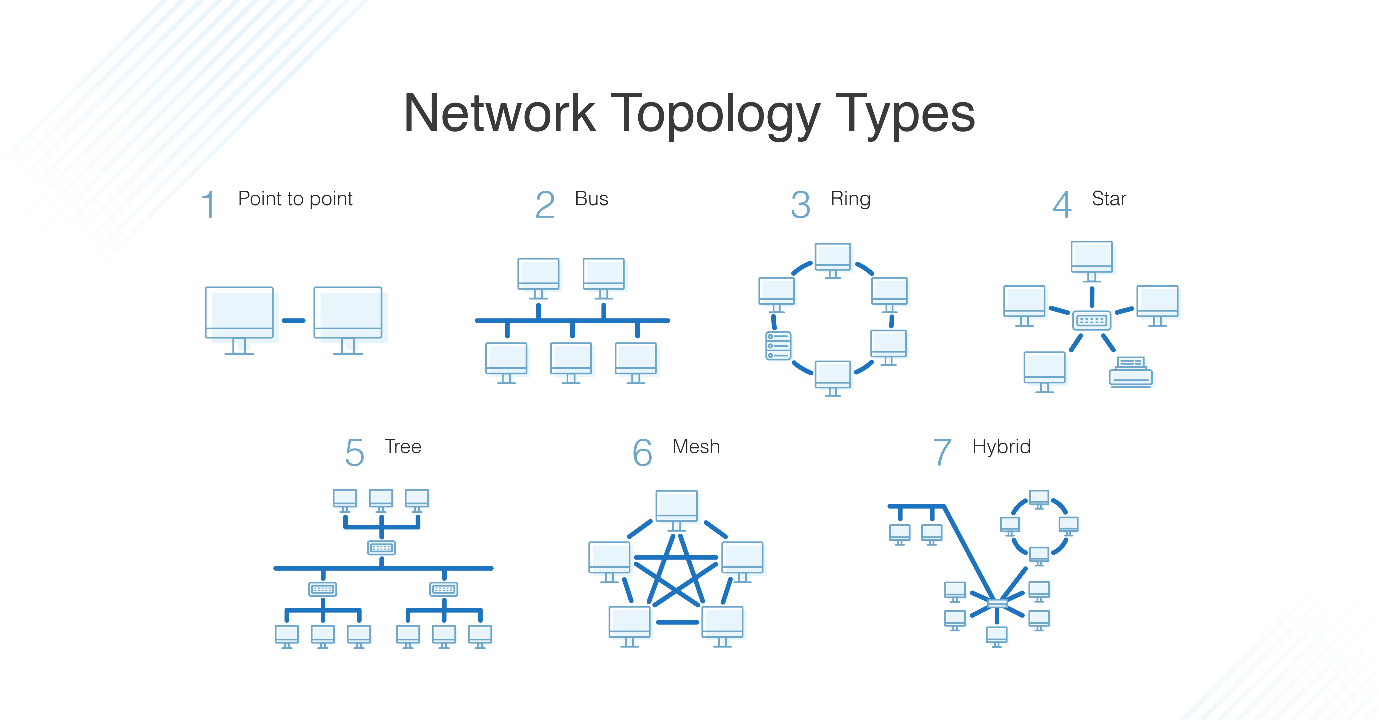
[Appendix 8](#_Toc39325007)

[Spaces By Department 8](#_Toc39325008)

[Floorplans 9](#_Toc39325009)

[Layered Network Diagram (Using Server VLANs) 0](#_Toc39325010)

# Problem Context

The Engineering and Computer Science department are getting an extension to their building and have given detailed floor plans as found in the appendix. 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 will be achieved by constructing a network and recommending a network topology that suits the building, 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 as seen in Figure 1.

*Figure 1: Network Topologies*

Each topology has its own advantages and disadvantages however, 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 chosen network must allow for wireless communication 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 chosen 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) employees. Once a topology is selected 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. A copy of all the spaces in the building can be found in the appendix, however there are 59 Engineering spaces, 48 Computer Science Spaces and 1 Pooled Computer Lab. There is also a comms room which should act as the main entry point/egress layer to the network.

Not all of these spaces require direct connection such as storage however the building should have wireless connectivity so should allow for connection in these rooms. Also, of note are the devices scattered around the building that are not associated to any department but should be connected, these are devices like printers. Many networking techniques will be deployed to ensure redundancy such as having multiple links with Scanning Tree Protocol (STP) so ensure packet efficiency. Security will be ensured by adding firewalls and other network-based solutions.

# Solution

## Three Layer Network Design

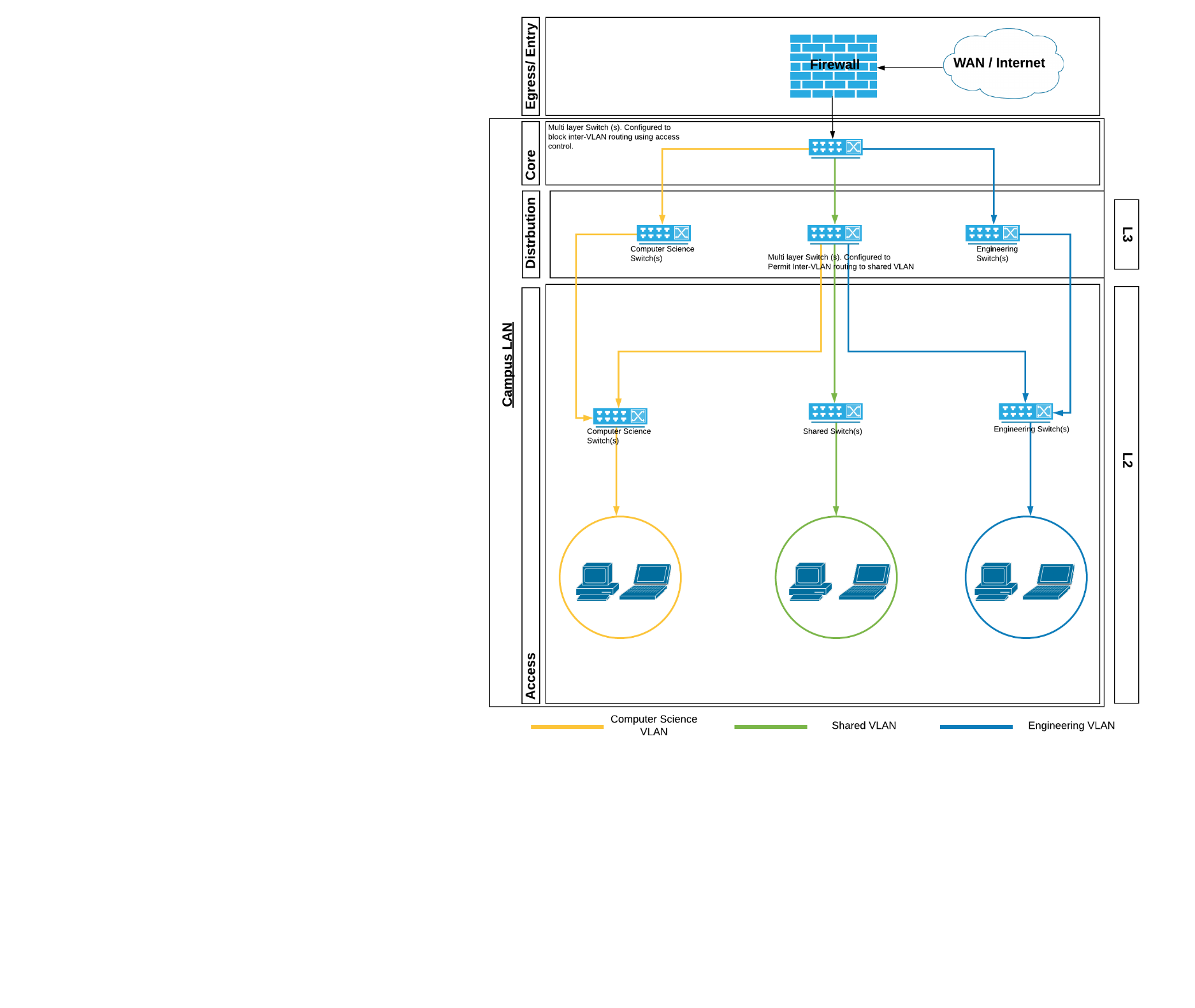
The network can be split up into three main segments, the core network which is the main processing for the whole environment. In this case this core network is likely to be part of the bigger network around the university. To ensure security from outside sources a firewall should be set up here before 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 or L3 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 having3 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 Level 3 switch/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/Multi-Layer Switch. This router/Multi- Layer switch 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 level 3 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 is to block them 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 L3 switch which supports VLANs, VACLs, Routing and VLAN Trunking. This split up network with the VLANs can be found in Figure 2.



*Figure 2: 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. 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, this acts as the main routing point around the entire network. This core level 3 switch must be configured to block inter-VLAN communication to ensure that all the devices remain segmented in the network but still have access to the internet. In the distribution section multi layered 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.

## Alternate Network Layouts

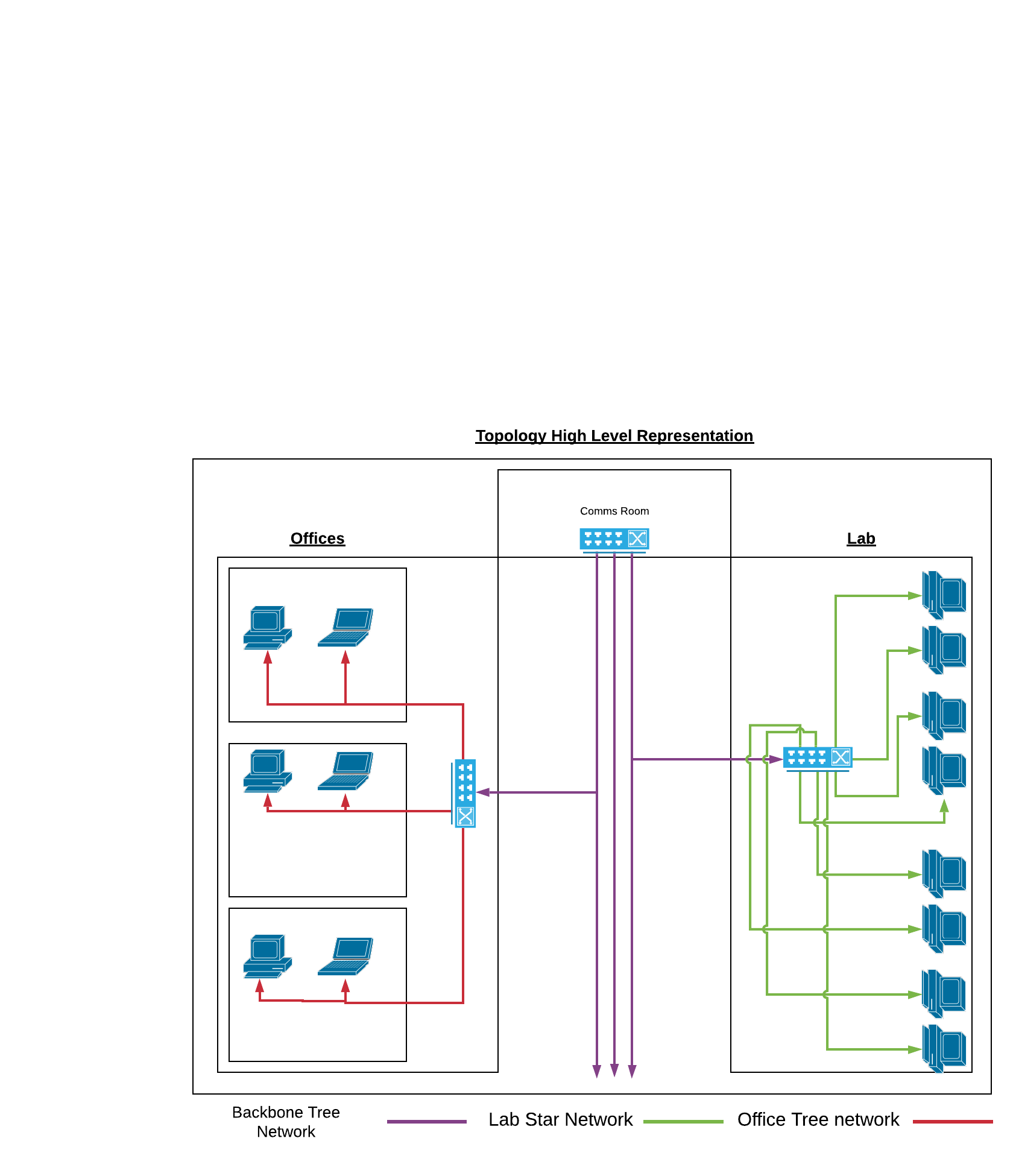
As mentioned there are alternates to this method, specifically the VLAN Merging method where the network VLANs are merged to create other VLANs. This requires the same amount of VLANs to the previous solution and could be harder to organise through the network, although it meets all the requirements. The basic principle is to merge the relevant server VLANs with the department VLANs allowing both of those VLANs to talk to each other on the same interface without the other VLANs having access. This uses the same limited multi-layer switch that Denys packets that attempt inter-VLAN communications. Other networking methods were thought of such as private VLANs however, no additional implementations that fully separated the network as required were found although there are definitely more that could be discussed using further advanced networking procedures. Efforts were made to use 3 VLANs but were unsuccessful without allowing full communications between VLANs using VLAN routing. It is possible to have 3 VLANs if the servers were not in the shared VLAN but that would not allow access to the resources that the shared area requires.

## 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. 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 3.



*Figure 3: Topology High Level Representation*

## Wireless

## Building Considerations

## 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

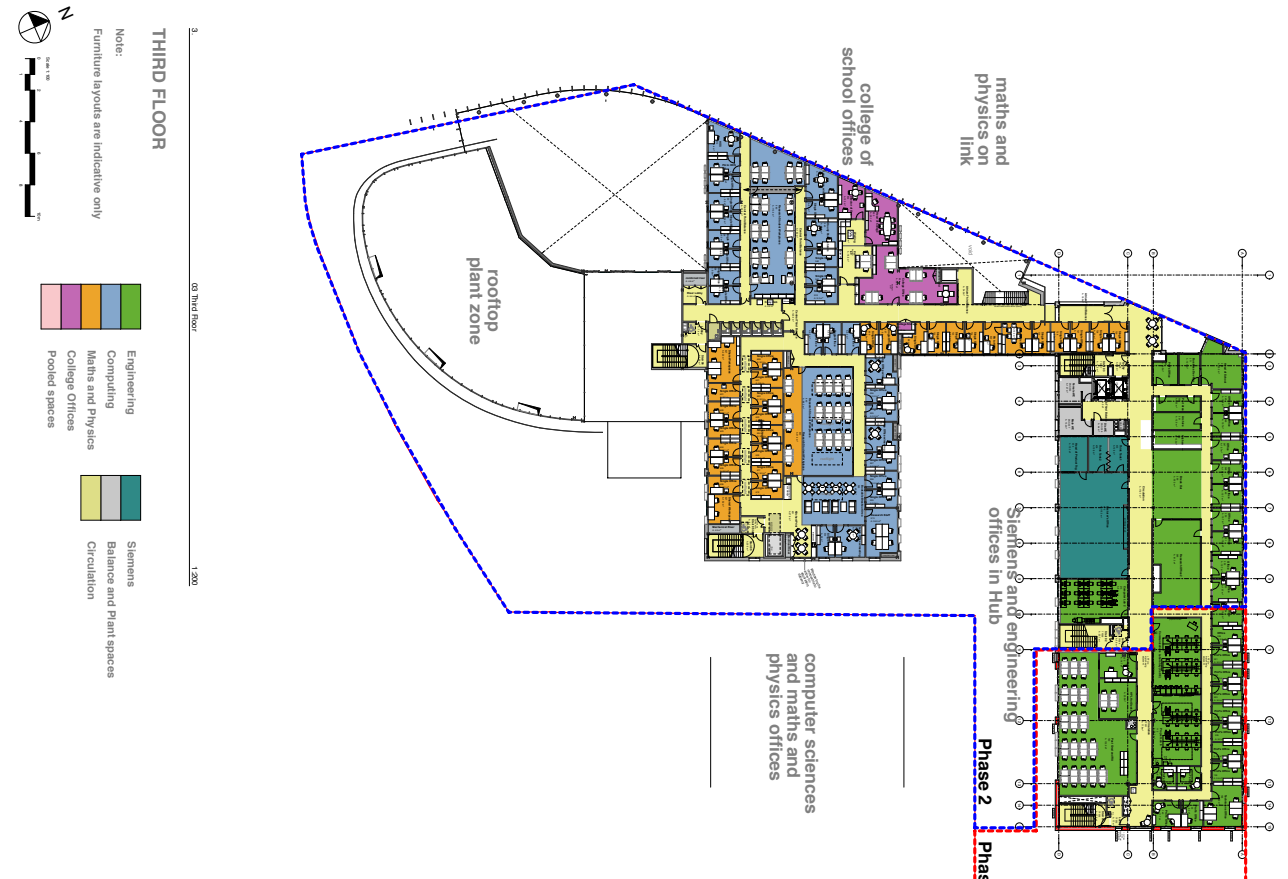
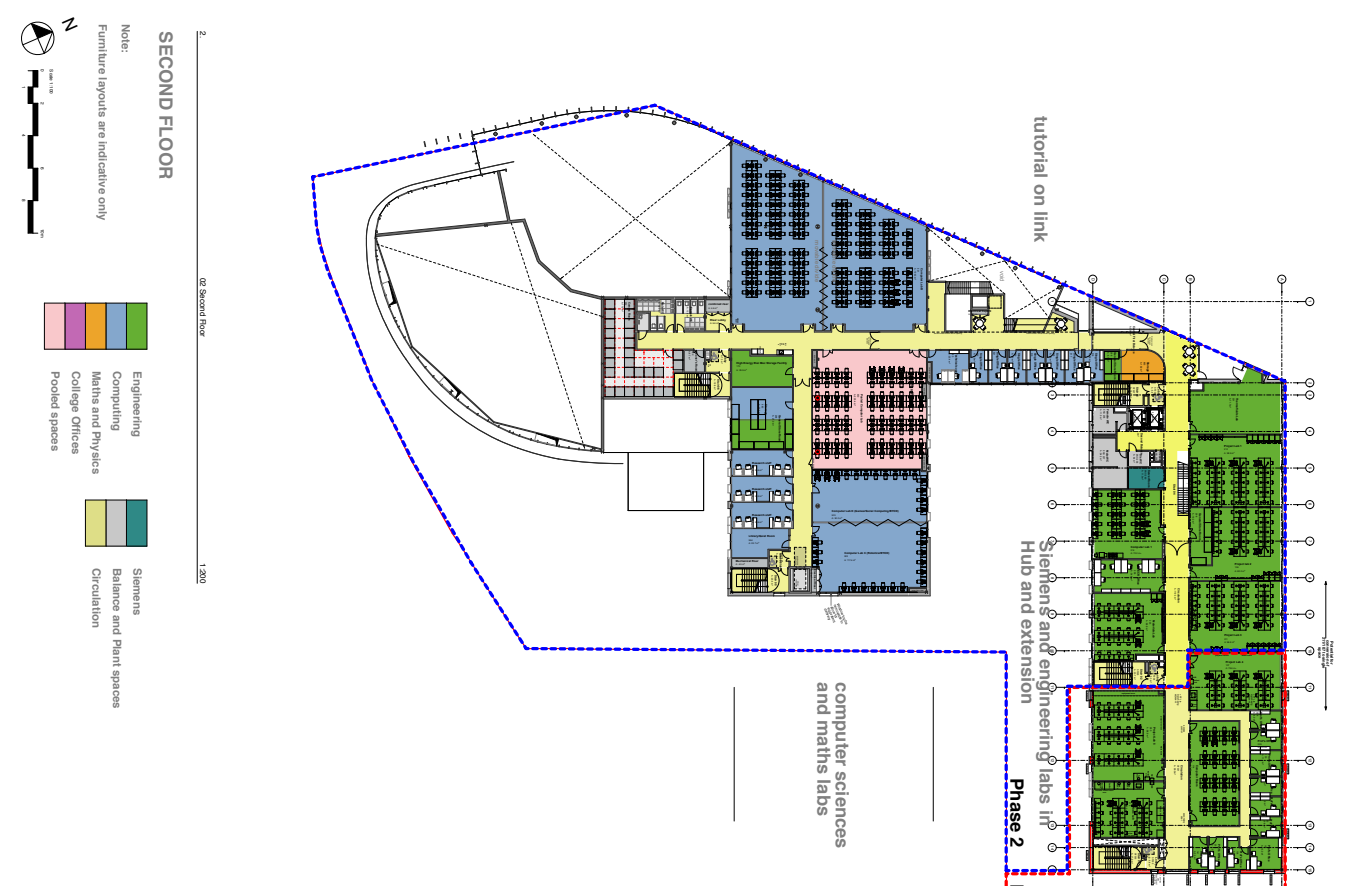
Cisco. (2018, May 6). *Chapter: Port ACLs (PACLs) and VLAN ACLs (VACLs)*. Retrieved from Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vacl.html

# Appendix

## Spaces By Department

|  |  |  |
| --- | --- | --- |
| Department | Room Type | Number of Spaces |
| Engineering | Professors Office | 23 |
| Engineering | Technicians Office | 1 |
| Engineering | Office | 11 |
| Engineering | Communications Laboratory | 1 |
| Engineering | Post Grad and RA | 1 |
| Engineering | HPL Hot Desks | 1 |
| Engineering | Project Lab | 6 |
| Engineering | Computer Lab | 2 |
| Engineering | Research Office | 1 |
| Engineering | Print Area | 1 |
| Engineering | Business Dev Mgr | 1 |
| Engineering | Head Of school | 1 |
| Engineering | Materials Lab | 1 |
| Engineering | ECR Office | 1 |
| Engineering | Computer Room | 1 |
| Engineering | Dr Fuels Lab | 1 |
| Engineering | Thermo fluids Lab | 1 |
| Engineering | General Store room | 3 (Including shared space) |
| Engineering | High Energy Elec Mec Storage Facility | 1 |
| Computer Science | Large Office w/meeting | 1 |
| Computer Science | Hourly Paid Lecturers | 2 |
| Computer Science | Single Office | 1 |
| Computer Science | Bookable Breakout Area | 4 |
| Computer Science | Research Student Workplaces(Joint with Maths and Physics) | 1 |
| Computer Science | PA to HOS | 27 |
| Computer Science | HOS | 1 |
| Computer Science | Technical support | 1 |
| Computer Science | Computer Lab | 1 |
| Computer Science | Storage | 1 |
| Computer Science | Research staff | 1 |
| Computer Science | Library/Quiet Room | 4 |
| Pooled Spaces | Pooled Computer Lab | (shared storage) 1 |
| Other | Linux Printer and Storage | 4 |
| Other | Copy Hub | 1 |
| Other | Printer | 1 |
| Other | Electrical Cupboard | 1 |
| Other | Comms Room | 1 |

## Floorplans



## Layered Network Diagram (Using Server VLANs)