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

**Contents**

[Problem Context 2](#_Toc39152757)

[Solution 3](#_Toc39152758)

[Three Layer Network Design 3](#_Toc39152759)

[Splitting up the network using VLANs 3](#_Toc39152760)

[Alternate Network Layouts 5](#_Toc39152761)

[Building Network Topology 5](#_Toc39152762)

[Wireless 5](#_Toc39152763)

[Building Considerations 5](#_Toc39152764)

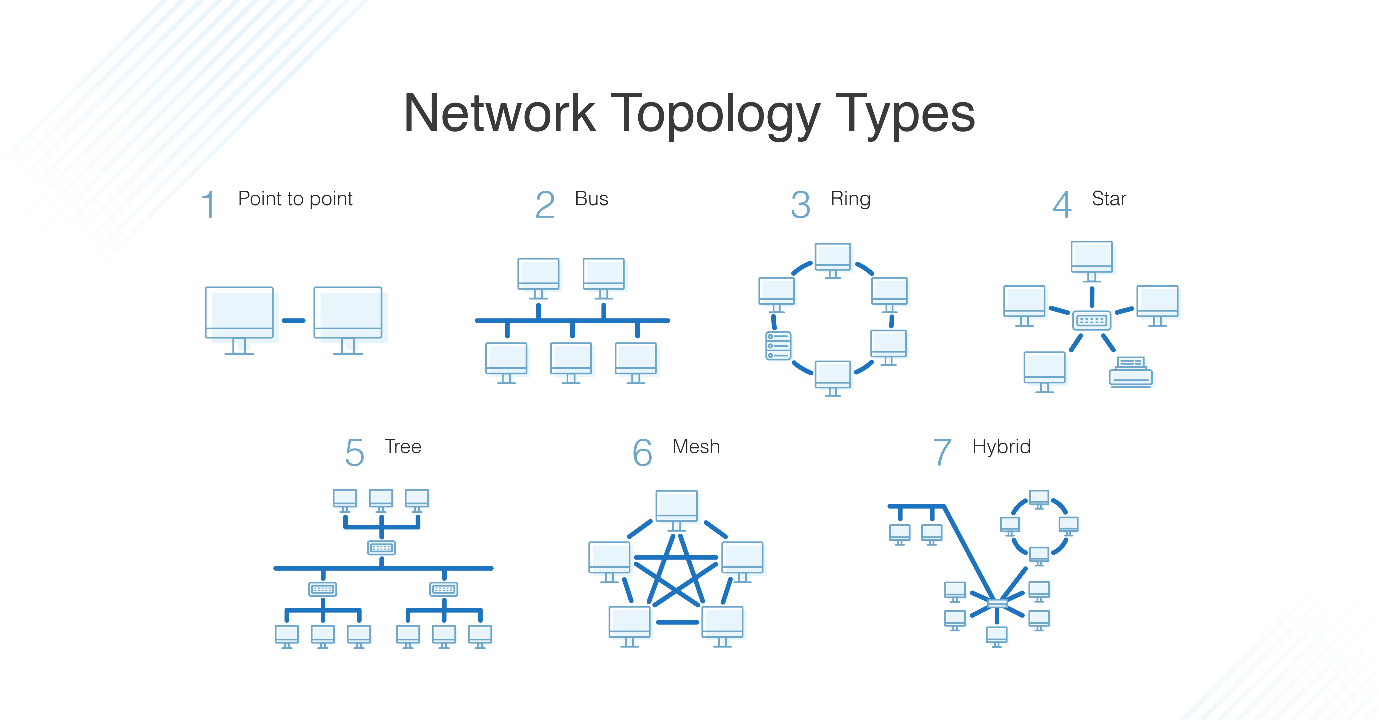
[Conclusion 5](#_Toc39152765)

[Appendix 6](#_Toc39152766)

[Spaces By Department 6](#_Toc39152767)

[Floorplans 7](#_Toc39152768)

# 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

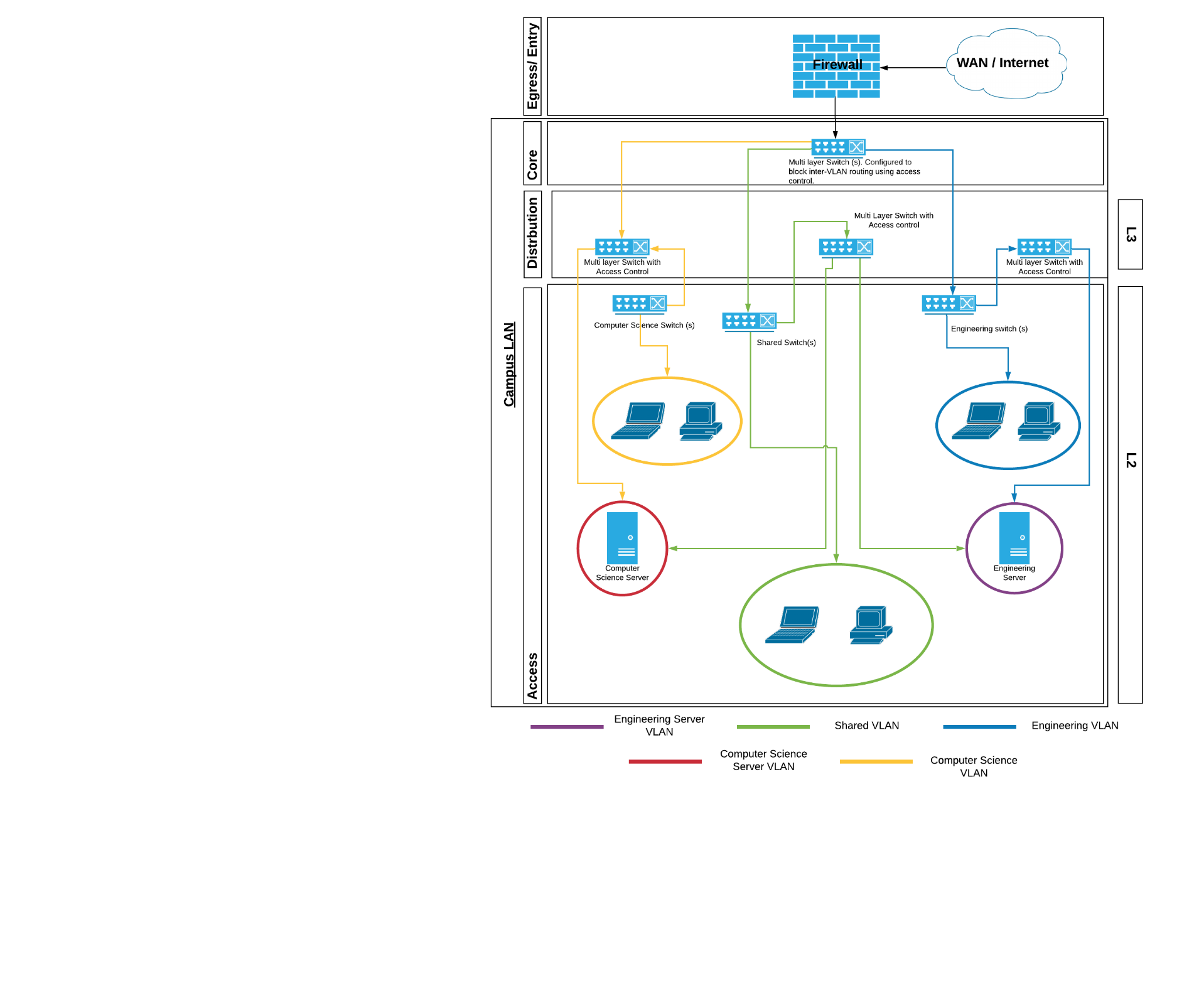
The network can be split up into three main segments, the core network which is the main processing for the whole environment. In this case this core network is likely to be part of the bigger network around the university. To ensure security from outside sources a firewall should be set up here before 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 having 5 VLANs. These include Computer Science, Engineering, Computer Science Servers, Engineering Servers and a shared VLAN. The servers can be set up to VLAN route using an L3 router or a multiple layer switch so they can communicate with other computers on different VLANs, an example of this could be when a server wants to communicate with a PC on a different 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. It is worth noting that this will allow connections from any computer.

To solve this issue VLAN access control lists (VACL) (Cisco, 2018) can be set up to only allow certain IP addresses to access the server, this could then whitelist the VLANs required to access the server including the shared VLAN. The default action of these lists is to drop the packets that are not authorised to access the network, however these VACLs can be configured to perform different actions such as redirecting packets. These VACLs can be set up around the network if extra access needs to be restricted, specifically it will be able to allow the server VLANs to communicate with their relevant department VLAN but not allow connections from other departments. To stop VLAN routing in the core layer this can also be set up to block IP addresses and drop the packets so that the devices only have access to the WAN (Cisco, 2013). Once set up the departments will now have full access to their independent servers but not each other’s unless they are in the shared VLAN which contains all of the devices shared between the departments.

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. An alternate way to implement this VLAN solution would be to merge the server VLANs to the department VLANs and merge the servers and the shared devices together to create a shared VLAN.



*Figure 2: Layered VLAN Network*

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 each department and shared configured with access control to talk to the relevant servers in the access layer. Finally, in the access layer all devices are connected via their department switches and routed to the Level 3 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.

## Wireless

## Building Considerations

# Conclusion

# 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

