Computer Systems Infrastructure and Management

600099

Network Infrastructure

Configuration Report

Brian Davis

Student ID: 201707824

Contents

[Problem Breakdown TODO-REWRITE 2](#_Toc39825560)

[Solution 3](#_Toc39825561)

[Network Design 3](#_Toc39825562)

[Using VLANs for the Network 3](#_Toc39825563)

[Building Considerations 5](#_Toc39825564)

[Designing the Network Topologies 5](#_Toc39825565)

[Wireless Functionality 6](#_Toc39825566)

[Deployment 8](#_Toc39825567)

[Selecting Devices 8](#_Toc39825568)

[Cabling Considerations 8](#_Toc39825569)

[Costing Breakdown 8](#_Toc39825570)

[Physical Deployment 8](#_Toc39825571)

[Logical Deployment 8](#_Toc39825572)

[Conclusion 8](#_Toc39825573)

[Bibliography 9](#_Toc39825574)

# Problem Breakdown TODO-REWRITE

The task involves the development of a network infrastructure for the University as part of their new building expansion. The main point of interest for the expansion is to incorporate a relevant and efficient network topology that aims to serve and connect the Engineering and Computer Science departments, by providing expansion upon their already existing building.

The university spans over 2 floors. There is need to develop a network solution that allows a connection across the different departments, where Computer Science and Engineering share spaces amongst the building. A network needs to be developed and plotted that aims to suit the requirements of the building as well as meeting the requirements of both departments. This will be achieved through a suitable, relevant, and efficient network topology that allows the requirements to be met. The network topology chosen must meet the requirements of the internal structure. An example of some topologies that are available to be used for this can be found in figure 1.

For this, consideration needs to be taken for the density of the pooled spaces, capacity of offices and the potential for wireless connectivity, which will allow expansion across the entire space. The two departments require their networks to be separate but to also be able to connect and share resources with each other across the pooled space. This connection needs to be available not only for local computers, but where necessary this must also cover the needs of those who use their own devices in the workspaces available or across the campus local area network.

The network infrastructure solution must allow for the ability to support activities within the computer labs, even when these labs are at capacity. This means that a fast connection needs to be available and that maximum through-put needs to be considered, but the likelihood that the full potential of network bandwidth will be used is not high. Mitigation to allow for this should be in place, to allow for no issues in lab use where capacity is expected to be higher than normal, especially in times of deadlines for coursework submissions. Due to the location of the comms room, a high speed wired connection needs to be available throughout the building that can suitably provide power and connection across the entire space.

The comms room can be found towards the south side of the building and consists of a long spanning corridor with only one entry and exit point along an outer wall. The corridors span the length of the floors and allow for ample ability to get everywhere, with no visible issues that can be seen from the floor plans regarding navigation.

To meet the requirements, the proposal is for a three-tiered network topology to allow for easy connection through the building, alongside allowing for future building expansions if these are deemed necessary later down the line. The corridors allow for Access Points to be situated in corners so that their connection can travel effectively through spaces without much interference or issues with walls effective connection quality.

The aim is to theoretically deploy the chosen topology to discover what resources will be needed and to gauge expected costs for this expansion. This includes the wiring, devices and additional network equipment that might be needed. Not all spaces within the building are expected to require a physical connection, but the building should have a wireless solution available throughout which is something to cover near the end of the report.

# Solution

## Network Design

The network will be split into three main segments which are the Core layer, Distribution layer and Access layer. The Core layer is the topmost part of the network that connects to an external firewall and is the backbone of the entire network. This layer allows for connection to the outside world and as such, the necessity for a firewall is key in keeping the overall network safe from potential threats from outside. The core layer needs to be designed with high availability and reliability in mind, and a fault tolerant design needs to be considered as well. Any failures need to be sure to have a minimal impact on the network and its connectivity. [three-tier-hierarchical-network-model.php](https://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php)

The second layer is the Distribution layer, which operates on the L3 band, and connects all the switches that will be deployed, to ensure that redundancy exists for the network. This layer defines the policy for the network and ensures that packets are delivered to the correct end devices and lays the foundations for connection to the lower Access layer. The required topologies for the network will be laid out in this layer before any connections can be made for the system. The Access layer, which operates on the L2 band, is where all end level connections will be made to the Distribution layer, for end-devices such as Computers, Printers and Mobile Devices.

## Using VLANs for the Network

To set up the network so packets go to the correct place and allow departmental network separation, Virtual Local Area Networks (VLANs) can be used. This solution is used, as it is possible to have the departments on the same physical network or subnet, whilst separating them into multiple logical portions that act as individual networks. This is done by ‘splitting’ connected devices and only allowing them to connect and talk to other devices on the same VLAN.

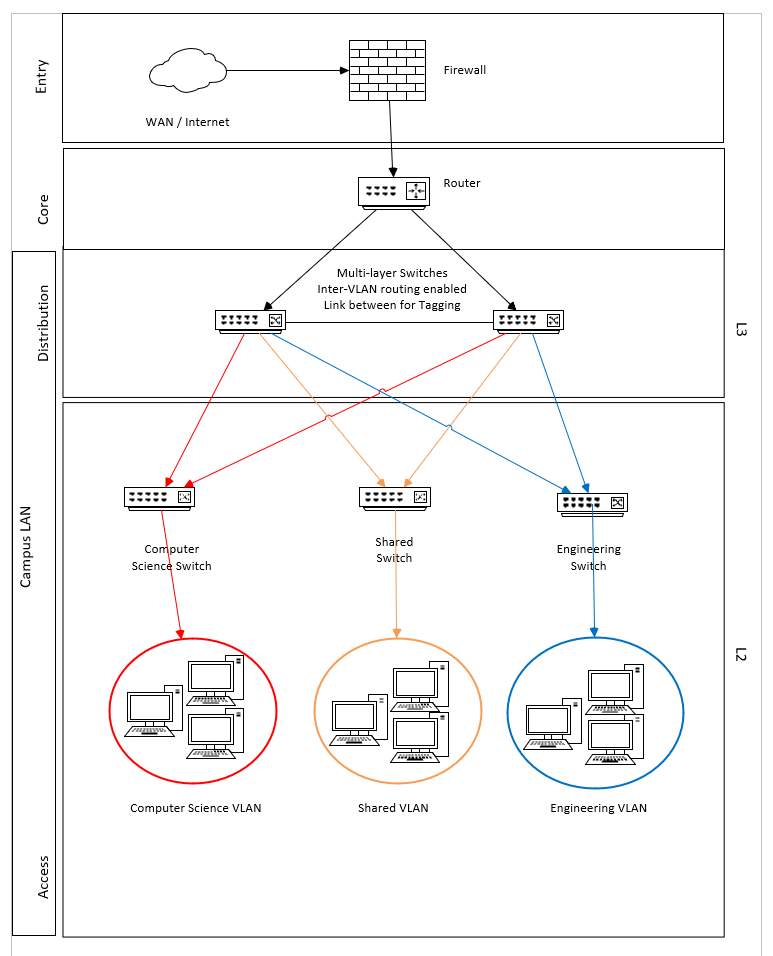
For the network traffic, it is possible to use a switch which can utilise VLAN trunking to create a single virtual link that all VLAN data can travel across. There are two types of VLAN configurations, which are port-based (untagged) and tagged [/how-do-vlans-work/](https://www.inteltech.com/blog/how-do-vlans-work/). Using a tagged VLAN allows for multiple VLANs to be configured using a single connected trunk port from one switch to another. This is done through a single connection to both physical switches using a single cable. Using VLAN tags across the trunk port on each switch allows for separation of VLAN A and VLAN B traffic without any physical separation. An example if we have three computers, where one is connected to VLAN A and the other two are connected to VLAN B. The two computers on VLAN B would be able to talk to each other but not to the computer on VLAN A which would be isolated from them. The amount of VLANs needed for this solution is three. There will be a VLAN set up for Computer Science and Engineering, and a VLAN for the shared resources for the pooled areas.

There will be a connection to each departmental VLAN and a shared VLAN which will primarily be in use in the pooled areas and in the computer labs. This will be done through Level 3 Multi-layer switches that can act as a switch and a router at the same time through inter-VLAN routing. The technique of Inter-VLAN routing is effective to route traffic to each VLAN on the network so that packets get to their intended destinations and are not visible to the other VLANs present on the network. The multi-layer switch allows for the ability to achieve switching and routing in a single box. This technique can be achieved in three different ways, but for this network, the use of inter-VLAN routing through a multi-layer switch is the chosen solution. [/inter-vlan-routing](https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41260-189.html)

To limit connection and packets through the VLANs, VLAN Access Lists (VACLs) can be used. This can be activated on a level 3 switch to block or permit inter-VLAN communication. Access can be permitted or blocked using IP addresses, Mac Addresses or through specified allowed ports. The default action blocks packets, but it is possible to configure this to allow the forwarding of packets amongst other things. Using VACLs allows for the communication to shared through both departments but stops the departments from communicating with each other directly.

The most important thing to consider regarding VACLs is that each VLAN can only have one list and they are a list of permit / deny statements. Any issues with configuration due to their top-down nature can cause access problems or weaknesses. Using this method is expandable to the other departments in the building if there is ever a need to add the other departments to the VLAN configuration, but this method helps to isolate the VLAN network and achieve our requirement of network separation whilst still having a shared access area available.

<https://www.ciscopress.com/> <https://www.youtube.com/watch?v=p3SfeQTaaxw>

TODO – discuss this diagram, then put this diagram in the appendix unless there is enough space to put it here.

## Building Considerations

The floor plan has a lot of issues that are not possible to correct but are worth mentioning. First is the location of the comms room. Being located where it is leads to much higher cabling requirements due to its distance from the far-right side of the building. It would be better if this room were more central to allow for a much easier cabling strategy to be taken up. Next is the comms rooms location facing an exterior wall, which is bad because there can be issues later regarding damp or flooding which could easily cause network disruptions and cause damage to equipment. The mitigation to this issue is to use racks that don’t touch the floor and a suitable online UPS that allow for the ability to get equipment shut down in the comms room in any such event.

Lastly, the comms room is close to electrical interference, in the form of the electrical riser close by, and the lifts situated opposite to the server room. If this room were to be used later for expansion purposes with siemens, there would be potential issues due to the EMI problems that will be caused by these lifts being so close in proximity. The risers located in the pooled computer lab (pink room on the 2nd floor on the diagram) are useful to allow cabling to reach the 3rd floor. Cables are needed to connect the switches from the comms room to the switches for each lab space and for all access points for wireless connectivity. There are also lifts situated within walking distance of the comms room to get this equipment upstairs for deployment. There are also places to store equipment for later use, including the electrical cupboard on the third floor and the general storage rooms on the second floor.

## Designing the Network Topologies

There are three main areas of the building where there needs to be consideration towards which topology will work best and where. A single type of network topology is not ideal here due to the size of the building. Starting off, the best way to set up the lab spaces and main computer rooms will be through a 48-port switch for each lab, with two switches connected through tagging where needed. Due to the nature of this connection, a star topology will be the best network topology for these labs ([star-topology](https://computernetworktopology.com/star-topology-advantages-disadvantages/)). It makes sense to have such a connection here because of the nature of the layout of the labs themselves. Half or all the computers in a lab will be connected to a switch which will be the central connection point for all these computers on the network.

This topology has many advantages for the lab spaces, the biggest one being the cabling situation. As each individual computer uses a single cable to connect to the switch and the network, it means that if there are any issues with a computer, it is easy to trace this back to the cable or the port on the switch, whilst having no effect on other computers on the network. This topology also allows for ease of device control and makes management a lot easier, alongside being great for high speed transfer of data to each individual connection. There is also ease of network extension through this method, adding new computers to the lab would simply be a case of adding a new cable to an empty switch port.

The biggest issue with the topology is that if the switch goes down then essentially the entire lab goes down too. This can be mitigated through a backup switch, which would allow a swap if the switch dies, and all that is needed is the reconnection of all port cabling into the switch. Another downside is this topology choice requires a lot of wires for connectivity.

([tree-topology](https://computernetworktopology.com/tree-topology/)) For the smaller areas and office spaces, the best choice for these areas is the tree topology. This is the best choice here as the number of devices is expected to be low, but a wired solution of some kind needs to be available for the offices, rather than expecting these areas to be covered by a fully wireless approach. These switches will reside in the hallways in a false ceiling with cabling going to each individual room to offer a wired port for connection. This topology allows for further connections in the small space and is quite easy to manage should there be any problems with any connections here.

This topology is also a good choice to implement here as it offers easy maintenance and fault identification. It is a combination of star and bus topologies, but the feeling is that star topology alone is not suitable for this, due to the amount of devices expected to be in use, unlike the labs where it is expected many computers will be connected at one time. One of the problems of this solution however is that is more difficult to configure than the star topology is, and it also has the same issue as the star topology where a switch failure will cause a disconnection of the network connection. For the larger offices there is consideration for star topology, the same as what is implemented in the labs, but this depends on if there is need for it and should be decided when it is required.

The overall connection of the building is done through a partially connected mesh topology ([mesh](https://www.computerhope.com/jargon/m/mesh.htm)). This is done at the top level to make the network more secure to a drop out or equipment failure. This is achieved using two switches from the comms rooms that are connected through tagging, which allows for an inexpensive way to apply redundancy to the network. There are multiple connections to the switches located within each room, but these are not connected to each other which indicates the potential for a partial mesh solution here. Care needs to be taken to ensure that there are multiple connections from the comms rooms, to make sure the network is secure in case anything fails.

The big advantage there is regarding using mesh is that a failure of a device in the building will not cause an entire network failure and data will continue to be transmitted regardless of this. This style of topology is more costly and allows for a lot more redundancy within the network, but it has the issue of being a more difficult network to set up and will require more time to get up and running in the initial stages.

## Wireless Functionality

Wireless is necessary for the building, as it is needed to allow students to be able to connect and access resources when travelling around the building or when using their own devices in the study areas on the third floor. This wireless network needs to reside on the shared VLAN, this is because the people connecting to this network could be from either department or therefore being on the shared VLAN allows them to access resources appropriate for themselves. A WLAN controller will be situated within the comms room so that the multiple access points within the building can be managed should there be any issues that need to be resolved quickly. Every access point will be connected to the same Service Set Identifier (SSID) to allow for ease of connectivity between all access points in the network.

Being on the same SSID means that once a user has a connection, wherever they go in the building, this connection will remain no matter where they go as long as they are on the campus, this means there is no wireless interruption to service. Due to the hallways and their width, there must be consideration towards having omni-directional wireless antennae.

These broadcast their signal a full 360-degree radiation pattern, so that they have a large range and are not blocked much by walls or other thick objects that could impede connection quality. This ensures that connection is strong and that all access points are connected if they are nearby another access point, allowing for constant connectivity. There is also need for dual-band support. While 5Ghz is the new standard and has the best speeds, it also has a much lower working range than that of 2.4Ghz. There is also the problem that not all devices themselves support the 5Ghz channel, so if the choice were to only support the higher channel, it might lead to connectivity issues for older devices.

([how-wireless-mesh-networks-work](https://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm)). The wireless implementation will make use of the mesh topology to connect all access points together to be able to handle high levels of traffic. High levels of traffic is expected within the wireless network, especially when people are propagating the hallways, so this mesh network can help alleviate the traffic and allow the network to find the best route to the comms room based on the location of the user and which access point they are accessing from. As mentioned before, the mesh topology can survive and continue working even if a device breaks, which is great for a wireless solution, meaning that the other access points closest can take over the workload until the device can be fixed or replaced, leading to no expected network slowdown. The solution of a mesh topology also means less wired connections are needed for the solution, meaning money can be saved on cabling costs, but more access points will be required so that availability and connectivity is not adversely affected by this.

## Deployment

### Selecting Suitable Equipment

|  |  |  |  |
| --- | --- | --- | --- |
| **Equipment** | **Quantity** | **Price per Unit Inc. VAT** | **Reseller** |
| S5850-48S6Q 48-Port 10Gb SFP+ L3 Managed Ethernet Switch | 3 | £3,829.20 | FS |
| LC-LC UPC Duplex OM3 Multimode Fibre Patch Lead 2.0mm PVC (OFNR) 5m | 1 | £6.36 | FS |
| Ubiquiti US-48-500W UniFi 48-Port Layer 2 Managed Gigabit PoE+ Switch w/ 2 x 1GbE SFP Ports & 2 x 10GbE SFP+ Ports (500W) |  | £773.58 | Broadband buyer.com |
| Ubiquiti US-24-500W UniFi 24-Port Layer 2 Managed Gigabit PoE+ Switch w/ 2 x SFP Ports (500W) |  | £550.00 | Broadband buyer.com |
| Juniper Networks QSFPP-40GBASE-SR4 Compatible 40GBASE-SR4 QSFP+ 850nm 150m MTP/MPO DOM Transceiver Module |  | £42.00 | FS |
| UniFi UAP-AC-PRO up to 1750 Mbps |  | Approx. £120.10 | Direct |
| Juniper MX204-IR Router | 1 | Approx. £19,678.08 | It-market  .com |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

<https://www.fs.com/uk/products/36439.html?fbclid=IwAR0M4fO-LgOxLeC2Gat9WvKX1Prb8V4WPGsXYqgyXFNNwpfmvXiAqGfAYe4>

<https://www.it-market.com/en/juniper-mx204-ir1?var=6>

<https://store.ui.com/collections/unifi-network-access-points/products/unifi-ac-pro>

### Cabling Considerations

### Costing Breakdown

### Physical Deployment

### Logical Deployment

## Conclusion

CHOSEN SOLUTION – Task List

* 3 VLAN with access to shared resources multi-layer switch
* Inter-VLAN routing and traffic
* Cabling will be Ethernet PoE Category 6 (research more power over ethernet cables)
* Adjust logical topology diagram – done so far
* Consider physical topology diagram, probably not needed though
* Decide upon all required equipment
* Start to look at prices, shop around, find lowest prices, maybe in bundles as well
* No servers / compute resources necessary
* Consider through-put heuristics of the labs, they don’t need higher data rate of 1Gbps max
* Network equipment (switches, routers, multi-layer switch can achieve a combined effort)
* Switches require some sort of link aggregation / degradation support, consider this)
* Consider number of needed ports, attenuation, link aggregation, etc
* What about any additional equipment?
* How would this equipment be configured? Wifi coverage etc
* Remember to justify all choices in the report
* Consider costs, try and save, cost should be reasonable, if something is cheaper, why this equipment over that?
* Consider expansion possibilities later
* Research Backhaul (2.4Ghz & 5 Ghz speeds and sharing / split)
* Consider aspects of Wireless integration across a Campus LAN
* Dual band APs at a minimum
* Equipment for Comms Room

# Bibliography

**There are no sources in the current document.**

To connect the Core layer for this network, it is proposed to use a multi-layer switch, which is a device that can perform the functions of a switch as well as a router at fast speeds. This network device can operate at higher layers within the OSI model, rather than being limited to the Data Link layer at layer level 2. This device can route packets and look inside these packets to make sure they are routed to the correct destination.

The choice between a router or a multi-layer switch here comes down to business need. Normally a router is the best choice for the Core layer implementation and connection, but in this case the proposal of a multi-layer switch feels more ideal, as it allows for more ports to be accessible to the Distribution layer, alongside better network performance and VLAN segmentation.

One of the main requirements of the network is to allow for the ability to have the departments operating on their own inter-networks, but also allowing for resources to be accessible in shared spaces such as the labs and for wireless devices being used within the building or Local Area Network on campus. To allow for the ability to fulfil this requirement for shared resources within the network, alongside separate local networks for departments, the Core layer multi-layer switch will connect to two multi-layer switches found in the Distribution layer.

The Distribution layer is the layer that is located between the Core layer and Access layer in a three-tier network. The purpose of this layer is to provide a boundary definition by implementing access lists. This is done through inter-VLAN routing.

Two multi-layer switches will be located within the Distribution layer, with each of these connecting to each switch in the access layer.

The technique of Inter-VLAN routing is effective to route traffic to each VLAN on the network so that packets get to their intended destinations and are not visible to the other VLANs present on the network. The multi-layer switch allows for the ability to achieve switching and routing in a single box. This technique can be achieved in three different ways, but for this network, the use of inter-VLAN routing through a multi-layer switch is the chosen solution.

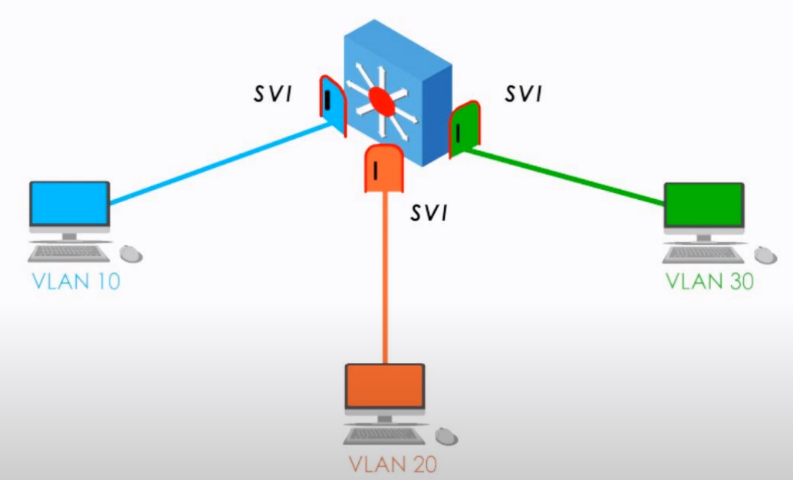
This is considered the best option as the multi-layer switch has the capabilities of a switch and router within a single box and makes use of switch virtual interfaces to act as gateways and perform routing.

Figure - Inter-VLAN Routing

The Switch Virtual Interface is important as it represents the interface on the L3 switch. This interface is important as it is needed to communicate with hosts in another VLAN. For this use case, the SVI will be configured to allow for traffic to be routed to the correct VLAN it is intended for, by providing a default gateway for each VLAN.

Trunking / Tagging is also something necessary to allow interconnection between switches. The switches are interconnected to establish these networks through trunking. These switches will have access ports alongside trunk ports, to allow the switches to share VLAN access and information between each other. This is also a good way to avoid problems later, where if one switch goes offline, the other switch can maintain the network until the problems are resolved.