Architecture, Operating Systems & Networking Report CA3

TU259

Oisín Fitzpatrick
C17448992

School of Computer Science
TU Dublin – City Campus

3rd May 2022

Table of Contents

Declaration

I hereby declare that the work described in this report is, except where otherwise stated, entirely my own work and has not been submitted as an exercise for a degree at this or any other university.

Signed:

Oisín Fitzpatrick

3rd May 2022

Chapter 1 - Introduction

For this assignment we have been given a case study for which we must develop and design a network plan. The case study involves an e-commerce company, which is expanding its operations into education, focusing on IT related disciplines. At the current time, it will offer course in computer programming. These needs may expand so 'future-proofing' of the design is imperative.

Network Design Requirements

The requirements of the design are as such; the building will have:

- ➔ 8 computer labs
  - 25 desktop PCs
  - A printer
- ➔ 4 Lecture Halls
  - 100 seating capacity
  - 1 Lectern
- ➔ 1 Library
  - 60 desks
  - 2 printers
- ➔ 1 Staff room
  - 20 hot desks
- ➔ 1 Open Plan Office space
  - 30 desks
- ➔ Campus Wi-Fi

For these overall requirements we have the following objectives:

1. Create a LAN for the campus
2. Create a network design and diagram
3. Design a subnet plan.

We must also select appropriate computer hardware for students to use through the facility. This includes the lab and office machines and potentially machines in the lecture halls and library.

Other amenities available to the students must also be accommodated and planned for. This includes a virtual learning environment (VLE), Moodle, and student drives, which will allow students to save their work on a single campus machine and access it from all machines on campus through their user login. As indicated, printing is also available to students and (presumably) staff, which will necessitate the inclusion of a printing server through which print requests can be sent and managed.

Summary of brief

This report will be conducted in four main sections, with an additional final conclusion.

We will begin with our background research, which will consist of a list of subsections. These subsections will include and discuss:

- ➔ Creating a LAN
- ➔ Network Components
- ➔ Protocols and Services
- ➔ General Hardware

Then the report will move to the network design which will be constructed from parts selected from the background research section. It will include a diagram that details the layout of the network, with additional information relating to cabling and network protocols such as DHCP, SFTP, DNS, and Active Directory within the design.

Continuing on, the operating systems use on any machines will be discussed, which may or may not include virtual machines/servers.

The final main section before the conclusion of the report will consist of the subnet plan and its justification, which will then be promptly followed by a brief conclusion.

Chapter 2 – Background Research

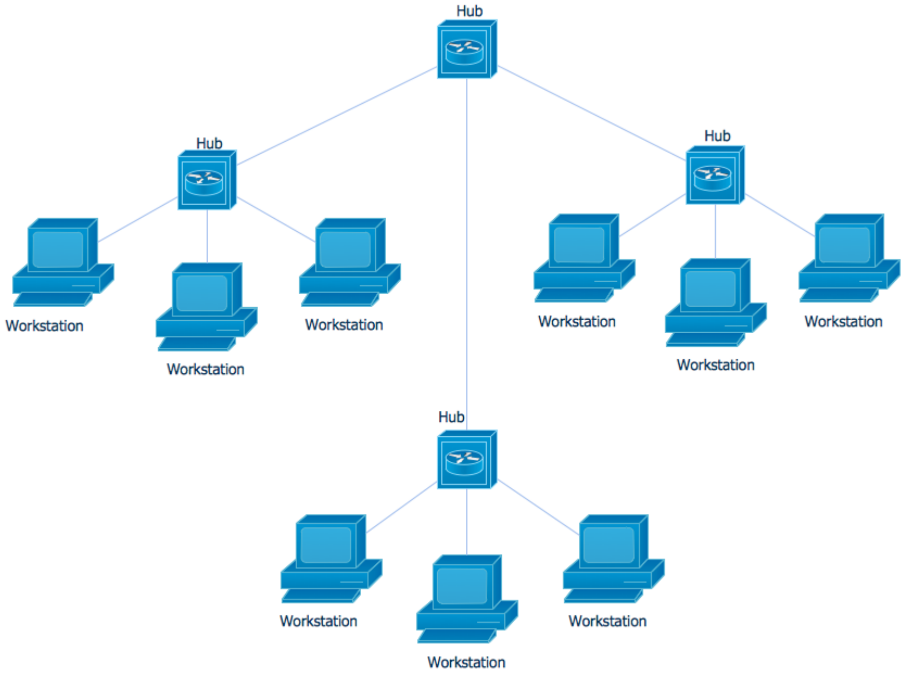
Creating a LAN

What is a LAN?

A good place to start would be to clearly define what a LAN is. A LAN (Local Area Network) essentially is a group of connected devices (network) within a single physical location (Local Area). This allows devices on the LAN to communicate with each other, or to a WAN (Wide Area Network) such as the Internet. The most common type of LAN is the client/server LAN model. A server is term used to generally describe machines that provide services to the clients on a network. Devices in the modern era can connect to a LAN through a wired or a wireless connection, which is facilitated by hardware and technology.
("What is a LAN?," n.d.)
("What is LAN (Local Area Network)?," n.d.)

What are network topologies?

A network topology is the structure of the devices and links between them. There are various types of topologies, which have different levels of effectiveness and popularity. The types include: Bus, Mesh, Ring, Tree, Star, and Hybrid. Of these the most common is Star Topology, which connects all devices in the network back to a central 'hub' device (not a literal Hub hardware device).



("What is Network Topology?," 2019)
(Conrad et al., 2016)
("Star Network Topology," n.d.)

How to Setup a LAN?

The general steps toward developing a LAN is to identify the services that will be used within the network including hardware, software, and amenities. These have been identified in the introduction of this report. A list of required hardware and analysis of product offerings available should then be conducted. A plan for the design of the network should be developed with a general overview of the physical layout of the network components clearly illustrated within comprehensive diagrams. This should follow the principles of a structured cabling system, which is detailed in the Cabling subsection. Then a subnet plan should be developed to understand the breakup and distribution of IP addresses within the network. The reason to do this is reduce amount of administration required to manage them. Following the purchases of selected hardware products, such as routers, switches, cabling, and access points, the physical installation of hardware should be completed, with necessary cabling and organization in place. After this, the necessary configurations of IP addresses and services, and installation of operating systems on server and client machines should be completed.

(“LAN, How to Set Up LAN Network?,” n.d.)

(NexGenT, 2017a)

(“What is VLAN?,” 2019)

Network Components:

Switches

A switch is a device used to connect other devices on a network by receiving and forwarding ‘packets’ of data from a source machine to a destination machine. Typically they connect multiple devices through the use of ethernet ports and drop cables.

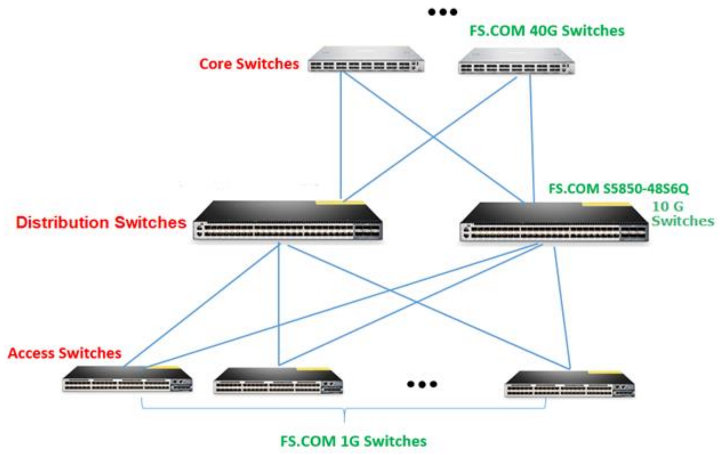
Of the OSI layers, most switches operate at layer 2, which is the layer responsible for translating data so that it may be used by the operating system of a machine and the network and vice versa. This layer is also responsible for encryption and decryption. In addition to layer 2 switches, there exist layer 3 switches. While layer 2 switches can only operate using MAC addresses, layer 3 switches can also function for static and dynamic routing. This allows a layer 3 switch to handle intra-VLAN communications.

(Moris, 2021)

In practical terms, there are two categories of switch to be concerned with in this report, these being Core and Edge switches. ***A core switch is typically a high-capacity, managed, and fast switch*** that acts as the gateway between a local area network (LAN) such as an office building, to a wide area network (WAN)/ Internet, allowing a connection to the internet using a router. It is the backbone of the network and all connections should lead back to the core switch. They are usually higher in cost over edge switches because they should have more features than an edge switch. Linking back to the previous paragraph, a switch device that will be used as a core switch should be a layer 3 switch.

On the other hand, an edge switch acts as an entry point to the network and, in typical use, is used to connect client devices i.e., desktops, laptops, etc. to connect to the network. Edge switches are not seen as critical pieces of the network, and so a tight budget can be eased by using a non-managed layer 2 switch for an edge switch. The mediator between the two is the distribution switch.

(Wong, 2017)



(Liu, 2018)

Switches Available

Moxa IKS-G6824A-4GTXSFP-HV-HV-T

This is a fully managed layer 3 switch with gigabit speeds with 24 ports. As of writing, it is being sold at roughly $5,500 by some retailers. This would make a good core switch, as being managed means that it can be configured better to suit the needs of the network by the administrator. It is also a standard 19 inch rackmount switch, which means that it will be neater and easier to manage. It can be configured to include SFP ports which would enable the device to connect via fibre optic cable.

TL-SG1048

This is an unmanaged layer 2 switch with gigabit speeds and 48 ports. It is approximately $500, which is a good price for such a device. Being a layer 2 switch, it would not be suitable for communications between vLANs, so it is not suitable to act as the core switch for our network. 48 ports is also enough to connect multiple devices such as lab machines, printers, access points etc.

Netgear GS348

This is another 48-port unmanaged, layer 2 switch, however it comes with a much cheaper price than the TL-SG1048 costing approximately $310. This may be a good choice for an edge switch, as it can function in the same way that the previously mentioned layer 2 switch, but at a much more effective cost.

Cisco Catalyst 1000, 550x and 9600 Series Switches:

Cisco is one of the largest providers of networking hardware and equipment, with some sources claiming they hold approximately 45% market share. ("Top 11 Most Powerful Networking Companies Across Globe -," n.d., p.). They offer many useful components such as switches. Of these, two product lines may be of use to our network. The Cisco 550X stackable managed switch offers 10Gb Ethernet capability with multiple ports, which can range from 24 to 48 of Gigabit and Fast Ethernet in the case of the SG550X and the SF550X. The 550X series are multilayer devices but are very affordable solutions with prices starting at only $639.00. These switches can be used to distribute connectivity to the core switches between groups of facilities within the same subnet. Additionally, the Catalyst 1000, which can have up to 48 ethernet ports can connect a lab, or other such facility, into the network as an access (edge) switch.
("Cisco 550X Series Stackable Managed Switches," n.d.)
("Cisco Catalyst 1000 Series Switches Data Sheet," n.d.)

For core switching, Cisco provides suitable products, which are highly configurable depending on the application, and so can vary widely in pricing depending on which modules are required. The 9600 platform can therefore be configured to suit the needs of our network.
("Cisco Catalyst 9600 Series Switches," n.d.)
("CATALYST 9600 Price, Cisco CATALYST 9600 GPL Price," n.d.)

All of the cisco switches series have models which are capable of gigabit speed uplinks.

Routers

Routers function as a device through which IP packets can be directed and communicated between different networks such as LANs or WANs. In order for the college to connect to the internet, it requires a router. Another term relating to routers is 'gateway'. A gateway is a network entity used within a network to facilitate communication with external networks. Its purpose is to act as the point through which a LAN connects to the WAN or internet. They can be viewed as protocol translators.
Routers operate at Layer 3 of the OSI layers. There are many categories of routers including enterprise and non-enterprise devices. These include, Wired, Wireless, Core, Edge, and Virtual routers.
Edge routers are usually found at the boundary of a network. In this case study, this will act as the gateway router for the campus.
(Howard, 2021)

(NexGenT, 2017b)
(Sarah Lewis and Burke, n.d.)
(Lutkevich, n.d.)
There is a plethora of devices available to use, and while it is important not to over-spend, subpar equipment will cost the company more. It is important that the router operates at gigabit speeds. The router within this network design is not intended to provide wireless connectivity, as this will be handled by the access points within a subnet. It is difficult to gather pricing estimates, as these units often come with custom configurations. They can also vary widely in their intended applications, depending on the overall size of the organization they are intended to supply, which leads to a great difference in pricing.

Cisco ISR 4461

Model	**ISR4461/K9**
Aggregate Throughput	**1.5Gbps**
Total onboard WAN or LAN 10/100/1000 ports	**4**
Total onboard WAN or LAN 10Gbps ports	**2**
RJ-45-based ports	**4**
SFP-based ports	**4**
Protocols and Services	**IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), RSVP, CDP, ERSPAN, IPSLA, Call Home, EEM, IKE, ACL, EVC, DHCP, FR, DNS, LISP, OTV[6], HSRP, RADIUS, AAA, AVC, Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IP sec, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE802.1ag, and IEEE802.3ah**
Rack Mountable	**Yes**
Price	**$16,766.00 router-switch.com**

Hewlett Packard Enterprise FlexNetwork MSR95x Router Series

Model	**MSR958 PoE (Power over Ethernet)**
Throughput	**146.48 Mbps (converted from 300 Kpps 64 Byte packets)**
Total onboard WAN 10/100/1000 ports	**2**
Total onboard WAN 10Gbps ports	**0**
RJ-45-based ports	**1**
SFP-based ports	**1**
Total LAN ports	**8**
Protocols and Services	**Layer 3 switching, Layer 2 switching, NAT support, VPN support, VLAN support, traffic shaping, port mirroring, Intrusion Prevention System (IPS), Weighted Fair Queuing (WFQ), Weighted Random Early Detection (WRED), sFlow, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, tunnelling, Access Control List (ACL) support, Quality of Service (QoS), Committed Access Rate (CAR), Link Fragmentation and Interleaving (LFI), PoE+, Unicast Reverse Path Forwarding (URPF), DHCP relay, Management Information Base (MIB), port isolation, packet storm protection, Class of Service (CoS), Loopback, Dynamic Virtual Private Network (DVPN), Multicast Border Gateway Protocol (MBGP), Ethernet over IP (EtherIP), Type of Service (ToS), Group Domain Virtual Private Network (GDVPN), random early detection (RED), ICMP Router Discovery Protocol (IRDP), Management Information Base (MIB) II, Source-Specific Multicast (SSM), OSPF, EGP, RIP, BGP-4, IS-IS, RIP-1, RIP-2, BGP, IGMPv2, IGMP, VRRP, IGMPv3, GRE, OSPFv3, Bidirectional PIM, MSDP, static IPv4 routing, static IPv6 routing, ECMP, RIPng, BGP-4+, MPLS, CIDR, BGP+, URPF, TCP/IP, UDP/IP, L2TP, RSVP, APPN, NTP, ICMP/IP, IPSec, AAL5, ARP, FTP, DHCP, PAP, SFTP, Secure Shell (SSH), RADIUS, PAP, CHAP, TACACS+, Secure Shell v.2 (SSH2)**
Rack Mountable	**Yes**
Price	**€1325.83 (elara.ie)**

Hewlett Packard Enterprise FlexNetwork MSR3000 Series

Model	**MSR3620-DP Router**
Throughput	**2.38 Gbps (converted from 5Mpps from 64 Byte packets)**
Total onboard WAN or LAN 10/100/1000 ports	**4**
Total onboard WAN or LAN 10Gbps ports	**0**
RJ-45-based ports	**4**
SFP-based ports	**2**
Protocols and Services	**Static IPv4 routing, Routing Information Protocol (RIP), Open shortest path first (OSPF), Border Gateway Protocol 4 (BGP-4), Intermediate system to intermediate system (IS-IS), Static IPv6 routing, Dual IP stack, Routing**

	Information Protocol next generation (RIPng), OSPFv3, BGP+, IS-IS for IPv6, IPv6 tunneling, Multiprotocol Label Switching (MPLS), Multiprotocol Label Switching (MPLS) Layer 3 VPN, Multiprotocol Label Switching (MPLS) Layer 2 VPN, Routing policy Spanning Tree Protocol (STP), Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping, Port mirroring, VLANs, sFlow, Define port as switched or routed WAN Optimization, NAT-PT, Address Resolution Protocol (ARP), User Datagram Protocol (UDP) helper, Dynamic Host Configuration Protocol (DHCP) Traffic policing, Congestion management, Weighted random early detection (WRED)/random early detection (RED), Hierarchical quality of service (HQoS)/Nested QoS, Other QoS technologies IPS, Enhanced stateful firewall, Zone based firewall, Auto Discover VPN (ADVPN), IPSec VPN, Access control list (ACL), Terminal Access Controller Access-Control System (TACACS+), Unicast Reverse Path Forwarding (URPF), Network login, RADIUS, Network address translation (NAT), Secure Shell (SSHv2) Internet Group Management Protocol (IGMP), Protocol Independent Multicast (PIM), Multicast Source Discovery Protocol (MSDP), Multicast Border Gateway Protocol (MBGP) Intelligent Resilient Fabric (IRF), Backup Center, Virtual Router Redundancy Protocol (VRRP), Embedded Automation Architecture (EAA), Bidirectional Forwarding Detection (BFD) HPE FlexNetwork Intelligent Management Center (IMC), Industry-standard CLI with a hierarchical structure, Management security, SNMPv1, v2, and v3, Remote monitoring (RMON), FTP, TFTP, and SFTP support, Debug and sampler utility, Network Time Protocol (NTP), Information center, Management interface control, Network Quality Analyzer (NQA), Role-based security, Standards-based authentication support for LDAP
Rack Mountable	**Yes**
Price	**$4,973.00 (shi.com)**

Cabling

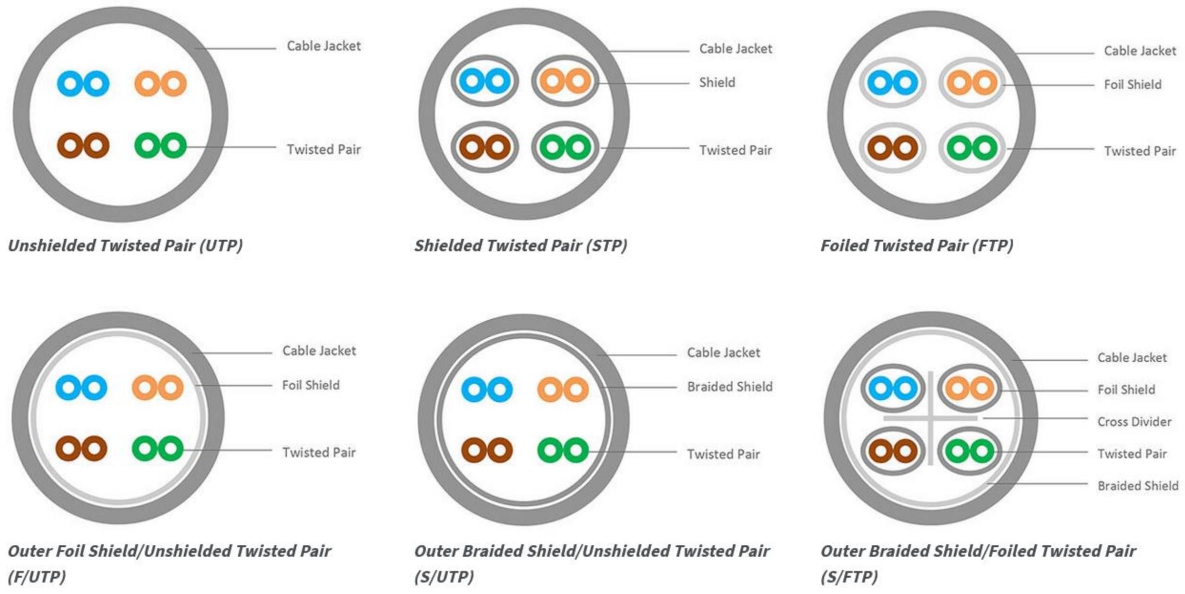
There exists many types and categories of cabling within networking. The major division within cabling is between Fibre Optic, coaxial, and twisted-pair Ethernet cabling.

Ethernet

Traditional ethernet cabling relies on the transmission of electrical signals through a length of copper wiring. There exist multiple categories (CAT) and types of ethernet cable. The different categories of cable can be used to generally gauge the data rate and bandwidth of a cable, and the max distance it can operate at. Most modern infrastructure uses CAT5 and above, with CAT5e being used in residential homes with a bandwidth of 1Gbps, a data rate of 100MHz, and a maximum distance of 100 meters, with extremes such as CAT8.2 used in core infrastructure having a bandwidth of 40Gbps, data rate of 2000MHz, and maximum distance of 30 meters. CAT6 is used in modern commercial buildings with gigabit internet. Its bandwidth is 1Gbps, with a data rate of 250MHz and a maximum distance of 100 meters.

Ethernet Cable Drawbacks

As touched upon previously, ethernet cables have maximum length for which they can be used. Above these distances, repeaters are necessary in order to preserve a signal. In essence, signal degradation due to the medium itself means that data cannot be ‘translated’ correctly by the time it reaches its destination. Ethernet cables. In addition to this, they are also vulnerable to electromagnetic interference which causes the aforementioned signal degradation. There are many types of shielding techniques that have been developed for this problem. These include Shielded Twisted Pair and Foil Twisted Pair. Certain categories have mandatory shielding techniques, for example, CAT7 cables must use S/FTP cables.


Cable Jacket
Twisted Pair
Unshielded Twisted Pair (UTP)
Cable Jacket
Shield
Twisted Pair
Shielded Twisted Pair (STP)
Cable Jacket
Foil Shield
Twisted Pair
Foiled Twisted Pair (FTP)
Cable Jacket
Foil Shield
Twisted Pair
Outer Foil Shield/Unshielded Twisted Pair (F/UTP)
Cable Jacket
Braided Shield
Twisted Pair
Outer Braided Shield/Unshielded Twisted Pair (S/UTP)
Cable Jacket
Foil Shield
Cross Divider
Twisted Pair
Braided Shield
Outer Braided Shield/Foiled Twisted Pair (S/FTP)

(“Ethernet Cables Explained | Tripp Lite,” n.d.)

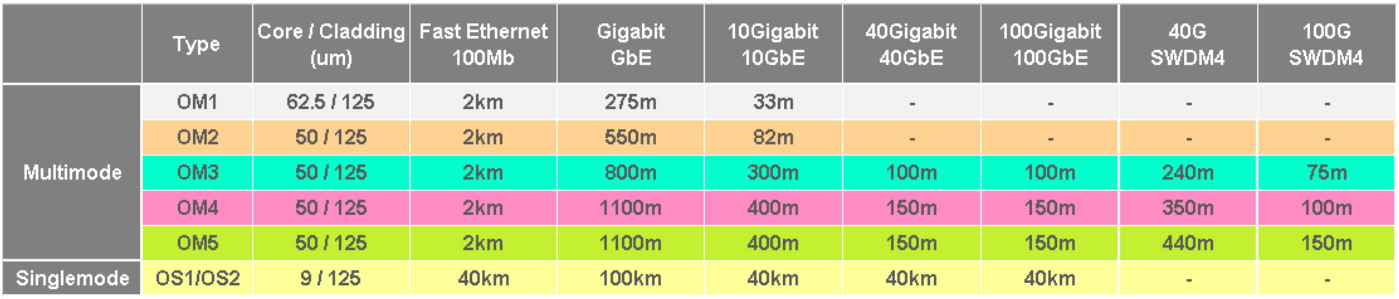
Choice of Twisted Pair Cabling and Price

For networks being designed with CAT6 cabling, the usual standards for cable are unshielded twisted pair (UTP) and FTP. Depending on the supplier, CAT6 FTP cables can cost around 50 cents per meter. It is recommended that business that are expected to grow should utilise CAT6 cabling, as it can be used for advanced applications, and has better performance than CAT5e cabling.
(“Common Types of Network Cabling For Businesses | LeadingEdge,” n.d.)
(“Cat6 FTP Shielded PVC Solid Cable | Cat6 Cable,” n.d.)
(“Ethernet Cables Explained | Tripp Lite,” n.d.)

Fibre Optic

Another type of cabling in use today is the Fibre Optic cable. Unlike the previously discussed Ethernet cable technology which relies on electrical currents for signalling, Fibre Optics, as their name suggests, rely on beams of light to send signals. Instead of using a medium such as copper wiring, Fibre Optic cables are constructed from fine strands of glass that are arranged to form the cable. Again, like Ethernet, there are different versions of Fibre Optic cabling available, mainly Single Mode and Multimode Fibre.

Single Mode fibres are the most basic, typically have thinner cores, and signals travel down the middle of the cable. Single mode cables find their use within internet and telephones. In contrast, multimode cables are much larger, and the light beam signal can follow multiple different paths down the cable. Multimode cables do not have the same distance capabilities of Single mode, in fact they can be orders of magnitude lower with certain bandwidths.



	Type	Core / Cladding (um)	Fast Ethernet 100Mb	Gigabit GbE	10Gigabit 10GbE	40Gigabit 40GbE	100Gigabit 100GbE	40G SWDM4	100G SWDM4
Multimode	OM1	62.5 / 125	2km	275m	33m	-	-	-	-
	OM2	50 / 125	2km	550m	82m	-	-	-	-
	OM3	50 / 125	2km	800m	300m	100m	100m	240m	75m
	OM4	50 / 125	2km	1100m	400m	150m	150m	350m	100m
	OM5	50 / 125	2km	1100m	400m	150m	150m	440m	150m
Singlemode	OS1/OS2	9 / 125	40km	100km	40km	40km	40km	-	-

(“Universal Networks,” n.d.)

As the chart above indicates, there are different standards of Multimode Cabling available. Mainly the difference revolves around their modal bandwidth.
(“Universal Networks,” n.d.)
(Bhaumik and McGrath, n.d.)
(“What Is Optical Fiber Technology, and How Does It Work?,” 2018)

Structured Cabling System

Besides the obvious hardware aspect of cabling, the way cables are terminated and the strategy for cabling within the building is also important to discuss and plan. This is known as a structured cabling system (henceforth referred to as a SCS). Within a SCS there are six subsystems: Entrance Facilities, Equipment Rooms, Backbone Cabling, Telecommunications Room, Horizontal Cabling, and Work Area.

Entrance Facility

This is typically where Internet Service Provider (ISP) cabling enters the premises, to the equipment room which connects the internal LAN to the WAN. This can often be located within the same physical room as the equipment room. This may include hardware provided by the ISP.

Equipment Room

As mentioned above, the equipment room contains the equipment that allows entrance cabling to connect the WAN to the buildings LAN. Equipment stored within the equipment room may contain core switches/routers, patch panels, gateway routers, and various servers. Often due to the sensitivity of the equipment stored within these rooms such as dedicated routers, servers, and switches, the environments of these rooms must be controlled so that temperature or humidity do not impact on network performance.

Backbone Cabling

This is cabling that links multiple floors of a building, which may involve connections between the entrance facility, equipment rooms, or telecommunications rooms. The previously discussed cables such as twisted-pair Ethernet, and single and multimode optical fibre cabling is used in backbone cabling.

Telecoms Room

This is another environmentally controlled room that contains the hardware that horizontal and backbone cabling terminate in, such as switches and patch panels.

Horizontal Cabling

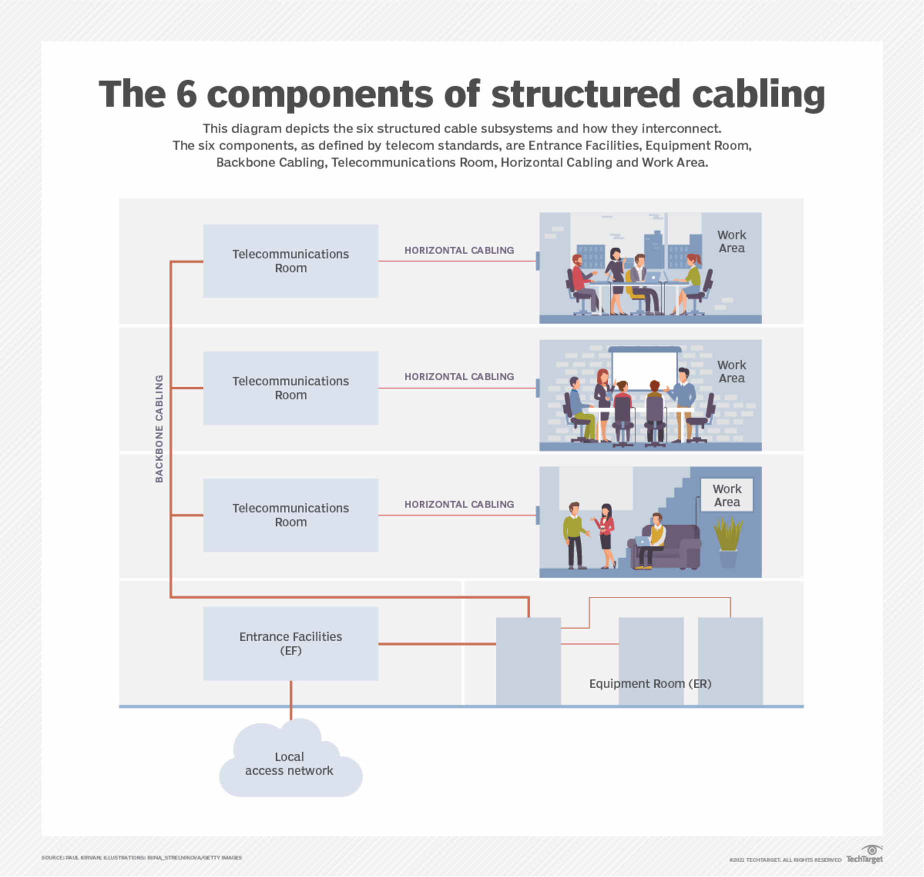
This is the cabling that typically connects workspace wall jacks/outlets to the telecom room on their floor. The maximum length according to guidelines for cable between a telecoms room and a workspace room is approximately 76 meters. The cabling used for this is typically the same as those used in the backbone cabling subsystem.

(“Telecommunications Horizontal Cabling and Support Structure - UIT | Montana State University,” n.d.)

Work Area

This is the area where actual user-end machines are located. They can use a switch or patch panel to provide wall jacks and connect client machines.

(Kirvan, 2021)



The 6 components of structured cabling

This diagram depicts the six structured cable subsystems and how they interconnect. The six components, as defined by telecom standards, are Entrance Facilities, Equipment Room, Backbone Cabling, Telecommunications Room, Horizontal Cabling and Work Area.

SOURCE: PAUL KIRVAN; ILLUSTRATIONS: IRINA_STRELNIKOVA/GETTY IMAGES

©2021 TECHTARGET. ALL RIGHTS RESERVED TechTarget

(Kirvan, 2021)

A structured cabling system will contain the following equipment, as described by Don Schultz:

- *‘‘Backbone cable running between floors or primary pieces of equipment (often fiber optic these days because it can go longer distances and is very high capacity)*
- *Copper Ethernet cable drops (also called runs) that are typically used on the same floor that run through the walls and above drop ceilings*

- *Outlet connectors mounted in or on walls (called keystone jacks) that are used to patch-in (connect) to the network with a patch cable*
- *Centralized patch panels where all the cable on the floor runs back to, so it can be patched into central Ethernet switches*
- *All of the support structure necessary to hold the cable in place like ladder rack, cable tray, conduit, and more"*

  (Schultz, 2022)

Cable Termination

The methods in which cables connect hardware pieces such as routers and switches necessitate the use of certain types of cabling is required. For example, in older systems, in order to connect two switches in sequence, the use of a crossover cable was required, however, modern switches and hardware typically feature Auto MDI/MDI-X ports which can automatically detect whether a crossover cable is necessary. With such systems straight-through cables can be used in place of a dedicated cross-over cable. In terms of connectors, a combination of 8P8C (commonly referred as RJ45) connectors and Copper SFP modules will be used. SFP modules are essentially hot swappable adapters for RJ45 connectors into different hardware and support up to Gigabit Ethernet transfer. For any Fibre Optic cables, transceiver modules will be required. Cisco offers the Cisco FET-10G module transceiver, which will allow the core switches to connect to sub switches within the LAN.

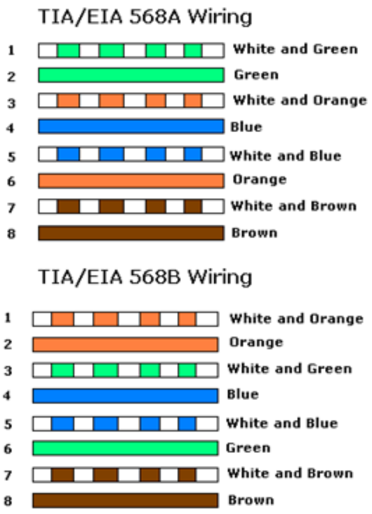


Figure A

Shows the Pin Out of Straight through Cables

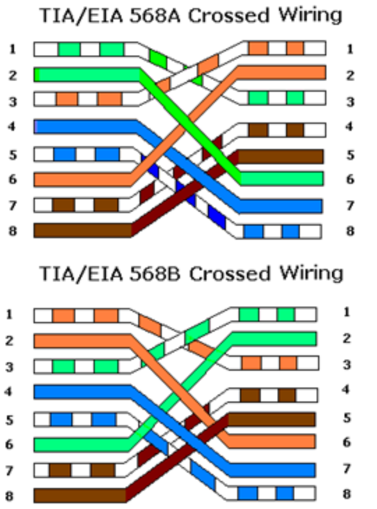


Figure B

Shows the Pin Out of Crossover Cables

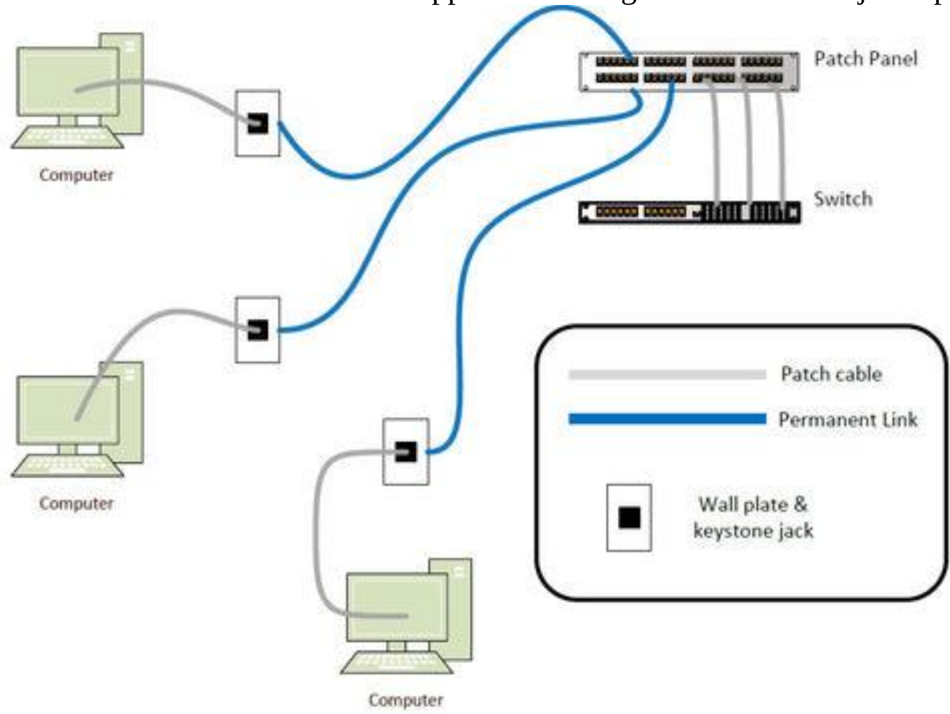
(Admin, 2018)
(Wang, 2017)
("What is Auto-MDIX feature in ethernet switches," n.d.)

Cabling of Choice

Of course, despite the amazing capabilities of Fibre Optics, the added costs currently make it less optimal than using CAT6 cabling for horizontal cabling purposes Additionally, Fibre Optics tend to be difficult to install and less flexible. For horizontal cabling, 1Gbps is still adequate, and this can be supplied with CAT6 cabling, however, this may change in the future. The network will use straight-through cables where possible. For backbone cabling
(Alice.Gui, 2015, p. 6)

Cable and Hardware Organization

Cabling will be organized using a combination of racking, patch panels, cable ties and other pieces of general cable management tools. Due to the large quantity of cables and hardware it is necessary for organizational equipment to be used, as this will enable faster and more efficient network maintenance and management. To simplify cabling throughout the facility, and using the structured cabling guidelines, hardware will be organized into centralized racking units throughout the facility. The standard rack mount size is 19 inches wide, with height usually measured in rack units (U), with 1 rack unit being equivalent to 1.75 inches. This height standard is typically seen on rack-mounted hardware listings (e.g., rack mounted switches) to quickly indicate how many rows of a racking shelf a piece of equipment will use. Racking depth has no single standard, but common racking depths include 24 inches and 48 inches. Racking shelves will be used throughout the facility to organize switches etc. To minimise the amount of cabling needed some racking shelves will contain a mixture of routers and switches, in particular the core switches and routers will be grouped together in a rack shelf, and the various server machines will be grouped together in the same rack shelf. When linking a telecom room to a workroom it is best to approach cabling with the rack-to-jack approach.



(Schultz, 2022)

Within a racking shelf, cables used to link hardware is known as patch cables, which are typically pre-made by factories. Sometimes PoE (Power over Ethernet) is needed, for example with Wi-Fi Access Points. In such circumstances, the keystone jack or patch panel it is connected to is, in turn, connected to a PoE enabled switch or router device. In order to link keystone jacks within a workspace back to their respective telecom room, a permanent link cable is used instead of a patch cable. Patch cables are another name for crossover cables and are used to link similar devices i.e. two switches. Of course, as previously mentioned, plenty of modern devices do not necessarily require the use of a crossover cable and so can use normal straight through cables. Typically this would involve connecting a patch panel to a keystone jack.

("Server Rack Sizes," 2020)
(Schultz, 2022)

Access Points (Wi-Fi)

Modern educational and business facilities are designed with wireless connectivity in mind. This is due to the fact that modern technology has made internet enabled devices such as smartphones and laptops extremely common. Some of these devices have no physical port for them to link into a network and must rely on wireless networking technologies. The most common of these is Wi-Fi. Most modern routers have wireless connectivity, and through them, client devices can connect directly to a WAN. However, for a large facility, one router is not sufficient to provide area coverage for the entire location. As such, Access Points (AP) provide for this gap in functionality. While a router can be configured to run as an access point, a pure access point only allows for communication within a LAN and cannot directly connect to a WAN, needing to connect to gateway router to do so. APs can also be connected in sequence to a switch and then to a router. A common practice in business is to run all wireless technology on a separate VLAN. This can be for added security within the network. When setting up multiple APs within a LAN or VLAN in close physical proximity, it is important to ensure that they are operating on different radio frequency channels to improve network performance and capacity.

An important aspect to investigate when discussing wireless networking is the standard at which they operate at. The most powerful and widely available commercial option is IEEE 802.11ax otherwise known as Wi-Fi6.
(Nganga, 2022)
(Horowitz, 2022)
("What is the Difference Between Access Point and Router?," n.d.)
("How to: Assign 802.11b/g Access Point Channels," n.d.)
(Lawrence Systems, 2020)

Different AP Devices

There are many types of AP points to select from, and individual units can be rather expensive depending on the manufacturer. Despite the price, it is worth investing into high quality of equipment, as the majority of devices within the LAN will be connecting via wireless connections.

C9115AXI-x: Cisco Catalyst 9115 Series

Cisco also produces a line of access points for a variety of different needs, with varying configurations. The 9115 series of AP can range in price from but typically within the $1000-$2000 range. They support Wi-Fi 6 and can connect to the network with CAT5e and CAT6 cabling to support speeds of up to 5Gbps.
("Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Data Sheet," n.d.)
("Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Data Sheet," n.d.)
("C9115AXI-EWC-X Price, Cisco C9115AXI-EWC-X GPL Price," n.d.)

Aruba 550 Series

The Aruba 550 series indoor access points are a popular Wi-Fi 6 enabled AP for large and high density public venues, which make them very useful for an educational environment. They are powerful devices and support up to 1024 client devices per radio, containing two or three radios depending on their configuration. They are sold at a base price of $1895, with more detailed configurations increasing the price.
("Aruba Simplifies Enterprise IoT Adoption with New Automated Security and Next-Gen Wireless Solutions," 2019)
("Aruba 550 Series Wi-Fi 6 (802.11ax) Indoor Access Points," n.d., p. 550)

Firewall

Security is an important concern for enterprises, and educational institutions. Protecting employee, student, or customer data is of the utmost importance, and there are legal ramifications for improper security protocols under legislation such as the European Union's GDPR (General Data Protection Regulation). There are different methods available for maintaining network security, including hardware and software firewalls. Software firewalls can typically deployed with less cost and skill, and do not require any more space than is already being used, and have no environmental restrictions beyond the needs of the devices they are installed on. Software Firewalls are more flexible in the number of devices they serve, and their protection can be expanded to protect more devices.

Hardware Firewalls, in contrast, are physical hardware devices that require space, environmental control, and typically have higher costs than a software firewall for installation and management by skilled staff. Hardware Firewall Devices typically stand between the gateway (edge) router and the core router of a LAN. Unlike Software Firewalls, Hardware Firewalls are limited in the amount of devices they can serve, meaning that there is potential for a Hardware Firewall to become unable to handle expanding needs of the enterprise.

There is need for both Software and Hardware Firewalls within the company, as the former can deal with internal threats, whereas the latter functions as protection from external threats. As this is a network planning report, a Software Firewall will not be discussed as this is not fundamental to the physical layout and implementation of the network. However, a Hardware Firewall is important to discuss, as it must be compatible with other hardware on the network.

Cisco offers a wide range of rack-mountable Hardware Firewall devices. Two product series may be of interest, the Cisco Secure 3100 and 4100 series which cater to medium and large enterprises respectively. The 3100 series is optimal for this network as it is capable of handling the needs of the network, yet will not break the bank as a 4100 series firewall will. Depending on the model, the IPS throughput of the 3100 series can be up to 45Gbps, with Maximum Concurrent sessions up to 10 million. It supports multiple interface connections with RJ45 and SFP+ support. It is more than enough for the campus facility with capacity to expand.
(Harmon, 2019)
(Kazmeyer, n.d.)
("What is a Hardware Firewall?," n.d.)
("Cisco Firepower 4100 Series Data Sheet," n.d.)
("What is Software Firewall?," n.d.)
("Why You Need Both a Hardware and Software Firewall," n.d.)
("Cisco Secure Firewall 3100 Series - Cisco Secure Firewall 3100 Series," n.d.)

Protocols and Services

The college is also offering a variety of different amenities to its students such as the ability for students to save their work on college machines, a printing service, and will facilitating online learning through a virtual learning environment through a VLE, Moodle.

Student Drives and Storage

In order for students to have dedicated storage on lab machines, so that they can access their data on any campus machine, they need to have access to a server-side storage location. In order for this to be possible, a networking protocol known as Network File System or NFS could be utilised. Essentially, the NFS protocol allows client devices on a network, in the case of this report this would be devices such as lab computers, to access files stored within a dedicated server, either onsite, or through the cloud in the case of Microsoft 365 which uses Microsoft Azure, which supports NFSv4.1. NFSv4.1 allows for internet functionality through firewalls. Other examples of cloud-based file sharing are with Google Cloud Storage, which uses Cloud Filestore.
One downside to using NFS is that it is not as secure as other file transfer protocols. An alternative to NFS is SSHFS, otherwise known as SFTP. While technically slower than NFS, it is much better for security.

In addition to SFTP, the network could implement is Active Directory (AD). This is a directory service developed by Microsoft, which runs on Windows servers. Through this service network administrators can create server directories and manage permissions and network resources for all potential users on a network. In this scenario, a folder would be set up on a central server for each user as their network storage location, and using Active Directory, different users can be granted access to their directory.
("SFTP Server Active Directory | Tbsoftinc.com," n.d.)
(Kath, 2020)
(Jake, 2019)
("Network File System (NFS)," 2019)
(Foley, 2021)
(Chai and Gillis, n.d.)
(Anonygoose, 2018)
(Keller, 2021)
(Cohen, 2021)

(Loshin, n.d.)
(JasonGerend, n.d.)

This sort of system should be utilised in conjunction with a Roaming User profiles, which allows for Active Directory Domain users to access their documents and settings on all client devices on a network domain.
(Lorenzo, 2015)
("Roaming user profile," 2022)

On-site file and data storage is resource intensive and costly. Another solution can be found in cloud-based storage solutions which are widely accessible. Advantages to this would be virtually limitless resources as long as the company is willing to pay for them. Beyond the benefits in scalability, there is something to be said of cloud storage as a security benefit, as outsourcing storage to a service provider whose sole focus is on data storage services means that more effective security is likely to be invested into by the service provider. While local storage may be faster, it does not have the same flexibility of use or scalability that the college is likely to need as it expands in its operations to additional campuses.
("Moving away from a physical shared network drive," 2019)

For student storage we can use cloud solutions such as Microsoft Office 365, which provides other cloud supported services such as mail, document writing, video calling, calendar, in addition to their cloud storage solution, OneDrive. The benefit of using cloud-based solutions, is that it is generally more secure as companies such as Microsoft can invest more time into maintaining security. Also, these cloud-based services often run across multiple types of devices, allowing students to access their documents from virtually anywhere with sufficient internet connection.
(KwekuA, n.d.)

Printing Service:

A dedicated printer service should be set up to allow students to send print jobs to printers within the building, either internally from the LAN, or from other company campuses through a WAN. Each branch/campus should contain a print server, which client devices will send their print jobs to. There are a handful of dedicated printing protocols including Line Printer Remote/ Daemon Protocol (LPD/ LPR), RAW, and Internet Printing Protocol (IPP).
The best choice for a print server to use is IPP, as that supports access control, authentication, and encryption for security and can, as its name suggests, operate over the internet. It is used by over 98% of printers worldwide, allowing for greater choice in printing device.
("Wide Area Networks (WAN) Considerations | PaperCut," n.d.)
(Oliveira, n.d.)
("List of printing protocols," 2022)
("Windows Internet Printing Service - IPP - RDR-IT," 2019)

Virtual Learning Environment (VLE): Moodle

Moodle is the virtual learning environment chosen by the company to conduct their teaching operations. Modern education requires great mobility and flexibility in curriculum delivery and so VLEs have become widely popular in recent years, which in large part has been driven by the COVID 19 pandemic. For much the same reasons to use cloud-based student storage, a cloud-enabled VLE would be a tremendous benefit. It would offset the need for on-site servers to manage the service, greatly contributing to network security, and should needs arise, can provide for increased demand by students and staff. MoodleCloud plans start at only $120 per annum, but fully customised cloud solutions can be developed by certified Moodle suppliers, where contracting prices can be negotiated. These service providers can supply cloud-based Moodle implementations. A recommended supplier would be Titus, a UK firm that claims to have developed Moodle solutions to service up to 100,000 users. While the college could indeed develop its own cloud-based Moodle implementation, it is much better and cost effective to outsource this to an expert company with experienced developers.

The benefit to using Moodle as the VLE is that it is possible for a Moodle solution to be integrated with Microsoft Office 365 and Azure Active Directory, providing students and staff a centralized location to access course materials and other resources. Such integrations can be discussed with whichever Moodle service provider is chosen.
("How to Integrate Moodle LMS with Office 365?," n.d.)
(Sebastian, 2022)
(Li and Lalani, n.d.)
(Kiran, 2021)

DHCP and DNS

Within a network various network machines such as routers, servers, and client devices that can use IP require an IP address. In essence the Dynamic Host Configuration Protocol (DHCP), allows for dynamic allocation of IP addresses among devices on a LAN. In order to do this, a DHCP server should be installed on the network. Alternatively, for smaller networks such as a home or a small office, a router can be configured to act as a DHCP server. DHCP is useful as it allows flexibility in which devices are connected to the LAN. For example, mobile devices such as phones and laptops that will leave and enter the network can be accounted and prepared for, and do not to be manually added and removed from the Network by the network administrator. DHCP allows for the 'recycling' of IP addresses, so that once a device disconnects from a network, its IP address can be given to another client device.
(Fisher, 2020)
(Pedamkar, 2019)
("When to use a seperate DHCP server vs having router do DHCP?," n.d.)

Domain Name Server (DNS) is another protocol critical to our network. Like DHCP, most home routers either connect to an external, or are configured to act as a DNS server. The purpose of a DNS server is to resolve human readable website names into machine legible IP addresses. As such they are crucial for modern workflows, insofar as they are fundamental to internet connectivity. There are many benefits for a company or institution to setup their own LAN DNS server. These include better speed and efficiency, as well as blocking inappropriate websites from being loaded on an employee's web browser. There also exist DNS services such as Google Public DNS or OpenDNS, which can be configured onto a server machine.
(Notenboom, 2013, 2013)
("What is DNS?," n.d.)
(Rubenking, 2022)

General Hardware

Obviously, many different machines will act as end devices to this LAN. These include lecturer and student lab and classroom desktops, printers, and servers. As this is a network focused report, the machines chosen are not the central concern, so in-depth reviews are not necessary, however, a general overview of the machines should be provided.

Client Machines (Lab and Library Machines)

The machines that will be utilised by the students should empower in their learning. As such the machines should have resources that should be capable of running high intensity programs and tasks such as virtual machines. This is a common requirement within IT related disciplines, and as hardware continues to advance and software develops to require more computing resources, it is important to ensure that the chosen machines will be able to provide this utility into the foreseeable future. The most important features of the machine should be the CPU, Memory, and Storage components. For CPUs core number, thread count, and clock speed are the crucial factors. For RAM, while speed is somewhat important, the main concern is total capacity, i.e., how many gigabytes of RAM. Finally, as long as storage is supplied on a modern SSD with 512 GB and above of space, it is suitable.

The Dell OptiPlex XE4 is a suitable candidate for a lab machine. All its major components, as discussed above, either meet the standard or surpass current standards for machines. Its 12th generation Intel i7 CPU features 12 cores, a 25MB cache, 20 threads, and a variable clock speed ranging from 2.1-4.9GHz. This should be more than sufficient for performing intensive computing tasks when combined with the machines impressive 64GB RAM, which should be sufficient capacity for the foreseeable future. Its 512GB M2 SSD is not so impressive with its size capacity, but due to the widespread adoption of Cloud storage technology (that the college is likely to supply its students), the need for machine local storage is less critical than in previous years. Dell allows for the machine to be customised with additional features including a dedicated NIC (Network Interface Card), GPU (Graphics Processing Unit), and additional storage devices. With savings applied, this machine can be purchased for €2,260.

(“OptiPlex XE4 Small Form Factor PC,” n.d.)

Server Machines

Server machines will be crucial pieces of hardware on the network that will be used to provide, at minimum, DHCP, DNS, and Printing services to the network. As such they should be machines that are capable of handling near constant workloads to handle the large number of requests being received from users on the network. A cost-saving technique that can be used to reduce the amount of server machines, is to use virtualization. With Virtual Servers, multiple different virtual servers can operate on a single physical device. To facilitate this a machine that has sufficiently powerful components must be selected.
The HPE ProLiant DL325 Gen 10 Server such a device, with many configuration options, and even payment plans. Indicative pricing starts around €3400, with higher spec machines obviously increasing the cost.

Technical Specifications

Processor: AMD EPYC™ 7000 Series (Features depending on selected Model)
- Cores Available: 32, 24, 16, or 8
- Cache Available: 32.00 MB L3, 64.00 MB L3, 128 MB, or 256 MB
- Clock Speed: 3.2 GHz (Max Clock Depending on Model)

Maximum Memory: 2 TB with 128 GB TypeHPE DDR4 SmartMemory ECC
Storage Supported:
- 4 LFF SAS/SATA/SSD,
- 8 SFF SAS/SATA/SSD with Optional 2 SFF SAS/SATA/SSD or 2 SFF NVMe,
- 8 SFF NVMe with Optional 2 SFF NVMe or 2 SFF SAS/SATA/SSD

Supported Operating Systems:
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux (RHEL) 7.4

(“HPE ProLiant DL325 Gen10 server | HPE Store US,” n.d.)
(“HPE ProLiant DL325 Gen10 Server User Guide,” n.d.)
(“HPE ProLiant MicroServer Gen10 x3421 Windows 10 Driver Support,” 2020)
(“AMD-EPYC-Data-Sheet.pdf,” n.d.)

Printers

The physical printer device at minimum must allow for wired networking, and sufficient quality printing services to students. The HP Color LaserJet Enterprise MFP M681dh printer provides these services with support for wireless printing through Google Cloud Print 2.0, HP ePrint, and a selection of other providers. The printers throughout the facility will be connected to a print server based on the previously discussed machine.

(“HP® Color LaserJet Enterprise MFP M681dh (J8A10A#BGJ),” n.d.)

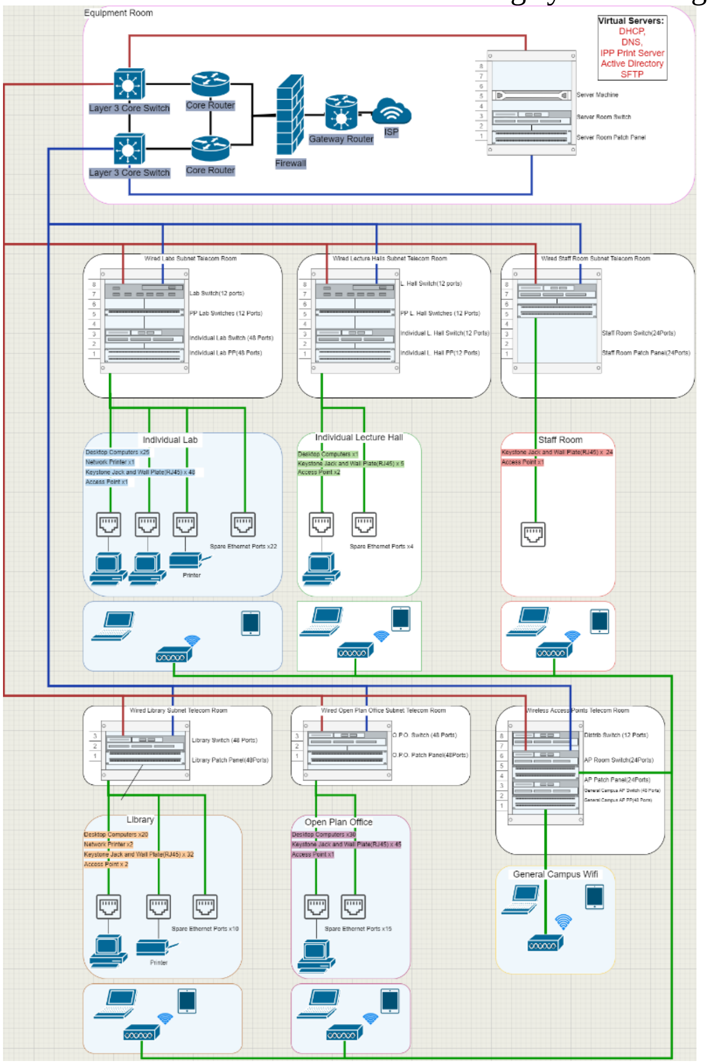
Chapter 3 – Network Design

The following diagram illustrates the entirety of the Network Plan. It is a high-level diagram that does not reflect the physical layout of the campus, but rather, a logical breakdown of the network. In the beginning of this report, an outline of the brief requirements of the network, highlighted the facilities and amenities that will be available to the students and staff of the campus. To reiterate, these are: 8 Computer Labs with 25 Desktop PCs and a Printer, 4 Lecture Halls with Seating Capacity of 100 (which presumably has a Desktop PC for the Lectern), 1 Library with 60 desks with 2 printers (Which may or may not include Desktop PC's), an Open Plan Office with 30 desks, and a Staff Room with 20 Hot Desks. With this information, we can begin with the breakdown of our Network Design.

Firstly, we need to break down the LAN into logical units. The most immediately obvious of which will be the various facilities of the campus. Of course, other categorisations may be used, such as by physical location i.e., floor level, however, this may lead to difficulty in management and administration of the network and its services. In addition to the student and staff facilities, the network also needs a server subnetwork where the network servers, namely the DHCP, DNS, Print and other possible servers that the campus may need, will reside. As such, the final list of Subnetworks are:

- Labs
- Lecture Halls
- Library
- Staff Room
- Office
- Server Room
- Campus Wi-Fi

Knowing this, we can use the various elements of structured cabling system to organise the network.


Equipment Room
Virtual Servers:
DHCP,
DNS,
IPP Print Server
Active Directory
SFTP
Layer 3 Core Switch
Core Router
Layer 3 Core Switch
Core Router
Firewall
Gateway Router
ISP
Server Machine
Server Room Switch
Server Room Patch Panel
Wired Labs Subnet Telecom Room
Lab Switch(12 ports)
PP Lab Switches (12 Ports)
Individual Lab Switch (48 Ports)
Individual Lab PP(48 Ports)
Wired Lecture Halls Subnet Telecom Room
L. Hall Switch(12 ports)
PP L. Hall Switches (12 Ports)
Individual L. Hall Switch(12 Ports)
Individual L. Hall PP(12 Ports)
Wired Staff Room Subnet Telecom Room
Staff Room Switch(24Ports)
Staff Room Patch Panel(24Ports)
Individual Lab
Desktop Computers x25
Network Printer x1
Keystone Jack and Wall Plate(RJ45) x 48
Access Point x1
Spare Ethernet Ports x22
Printer
Individual Lecture Hall
Desktop Computers x1
Keystone Jack and Wall Plate(RJ45) x 5
Access Point x2
Spare Ethernet Ports x4
Staff Room
Keystone Jack and Wall Plate(RJ45) x 24
Access Point x1
Wired Library Subnet Telecom Room
Library Switch (48 Ports)
Library Patch Panel(48Ports)
Wired Open Plan Office Subnet Telecom Room
O.P.O. Switch (48 Ports)
O.P.O. Patch Panel(48Ports)
Wireless Access Points Telecom Room
Distrib Switch (12 Ports)
AP Room Switch(24Ports)
AP Patch Panel(24Ports)
General Campus AP Switch (48 Ports)
General Campus AP PP(48 Ports)
Library
Desktop Computers x20
Network Printer x2
Keystone Jack and Wall Plate(RJ45) x 32
Access Point x 2
Spare Ethernet Ports x10
Printer
Open Plan Office
Desktop Computers x30
Keystone Jack and Wall Plate(RJ45) x 45
Access Point x1
Spare Ethernet Ports x15
General Campus Wifi

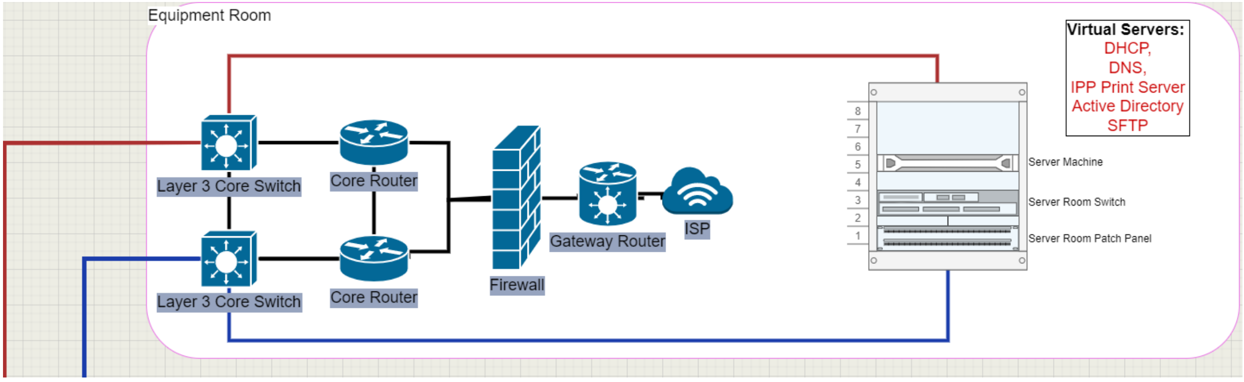
Entrance and Equipment Room

The entrance and equipment room will more than likely share the same physical location. The ISP leased line will connect via Fibre Optic cable into the gateway router. The gateway router is weak point within the network, so a Firewall should be used to insulate the internal LAN from threats attempting entry through the Gateway Router. Connected then through the Firewall to the gateway is the two core routers. The use of two core routers and subsequent core switches is to allow for redundancy, and in normal circumstance only one of each will be in use at any one time. This helps to virtually eliminate network downtime in the case of hardware failure. For both gateway and core routers, the Cisco ISR4461 will be used. In the event of hardware failure of the gateway router, the Firewall can be configured to act as the gateway, although this may not be possible depending on the needs of the network in terms of advanced routing requirements. For the Firewall, the Cisco Secure 3110 will be utilised. For the connections between the core routers, HSRP (Hot Standby Router Protocol) will be used to accommodate the redundancy system for the network should one router fail. In essence HSRP allows two routers to be seen as a single virtual router by the LAN, as they are grouped together as the so-called ‘standby group’. Only one router of this group is active at any one time and is responsible for normal routing functionality for the network.

(“Hot Standby Router Protocol Features and Functionality,” n.d.)

As indicated the core switches are the next hardware elements within the network sequence. These core switches will be customised configurations of the Cisco 9600 Series multilayer switch. These will also be connected together using STP (Spanning Tree Protocol), which performs in much the same was as HSRP.

(“Layer 2 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x (Catalyst 9600 Switches),” n.d.)
This same equipment room is likely to also house the physical server machines on the LAN, however, this does not change the logical layout of the subnet.



Backbone Cabling

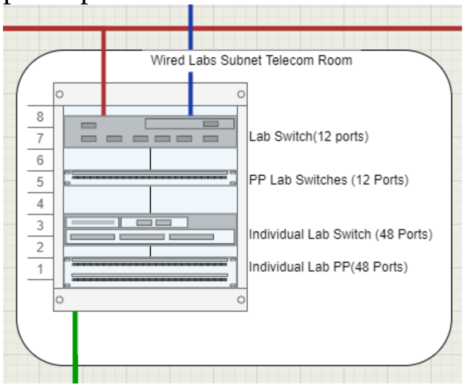
The where possible OM 3 & 4 cabling will be used to connect the Core Switches to the various telecoms room throughout the facilities, and the access switches therein. Of course, this will require transceivers to be installed, and may not be possible due to physical restrictions such as tight bends. In the event that Fibre-based backbone cabling is not possible, Cat 6e cabling should be utilised with standard RJ45(8P8C) connectors, and SFP modules should be used to connect core switches and access switches. In the diagram, backbone cabling is indicated by the red and blue lines, each representing a direct connection from each of the core switches to the distribution switches of each subnet.

Telecoms Rooms

Due to the unknown physical layout of the campus building, it is uncertain whether each subnet will have its own dedicated telecommunications room. It is more likely that there will be a telecommunications room for each floor which may house the distribution and access switches for each subnet in separate racking units, or even possible same racking units. For simplicity’s sake, this report continues with the assumption of individual telecoms rooms and racking units for each subnet, but this of course is just an abstraction, and is not to be implemented within the physical network. The distribution switches will be the Cisco 550x series multilayer switches with different configurations for their number of ports, and the access switches will be the Cisco Catalyst 1000 series switches.

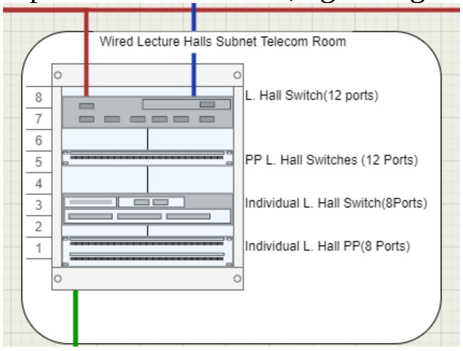
Wired Lab Subnet

The first telecoms room to be discussed will be the wired labs room. This will host a single 12-port distribution switch and eight 48-port access switches, one for each lab room. Between these two switches there will be a patch panel which will assist in the organisation of the network.


Wired Labs Subnet Telecom Room
8
7
6
5
4
3
2
1
Lab Switch(12 ports)
PP Lab Switches (12 Ports)
Individual Lab Switch (48 Ports)
Individual Lab PP(48 Ports)

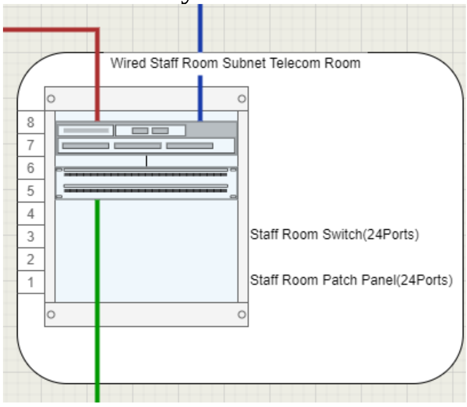
Wired Lecture Hall Subnet

Like the Lab Subnet, the Lecture hall telecoms room will contain a single 12-port distribution switch, and four 8-port access switches, again organised using patch panels of appropriate port number.


Wired Lecture Halls Subnet Telecom Room
8
7
6
5
4
3
2
1
L. Hall Switch(12 ports)
PP L. Hall Switches (12 Ports)
Individual L. Hall Switch(8Ports)
Individual L. Hall PP(8 Ports)

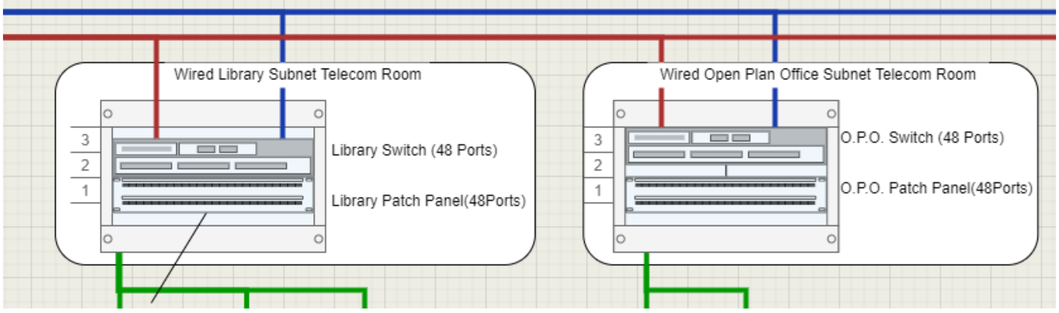
Wired Staff Room Subnet

Unlike the previously mentioned Lab and Lecture Hall subnets, only a single 24-port access/distribution switch is really needed to accommodate all the ports necessary for the hot desks in the staff room.


Wired Staff Room Subnet Telecom Room
8
7
6
5
4
3
2
1
Staff Room Switch(24Ports)
Staff Room Patch Panel(24Ports)

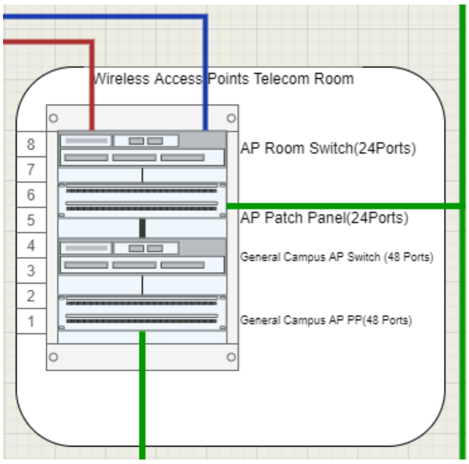
Wired Library and Open Plan Office Subnets

Like the previously mentioned Staff Room Subnet, the Wired Library and Open Plan Office Subnets only consist of a single 48-port access/distribution switch each, which are enough for the combination of PC and spare wall jacks for the Library and Open Plan Office each.


Wired Library Subnet Telecom Room
3
2
1
Library Switch (48 Ports)
Library Patch Panel(48Ports)
Wired Open Plan Office Subnet Telecom Room
3
2
1
O.P.O. Switch (48 Ports)
O.P.O. Patch Panel(48Ports)

Wireless Wi-Fi Subnet

The wireless network runs all on a single subnet, however, it is unclear the best solution for distribution of the network. For this network plan, the general guid was to break the wireless network into subgroups, room-based and general campus Wi-Fi. As shown in the full network diagram, each room has a logically separated wireless network using access points. In addition to these room-based AP, there are 'general campus' access points, which could potentially include, kitchens, canteens, hallways, or other 'general' intermediary locations within the building. The subnet consists of a 12-port distribution switches with a single 24-port access switch for all room-based APs, and a 48-port switch for the general campus Wi-Fi. The wireless access points chosen for the network are the Aruba 550 series access point.


Wireless Access Points Telecom Room
8
7
6
5
4
3
2
1
AP Room Switch(24Ports)
AP Patch Panel(24Ports)
General Campus AP Switch (48 Ports)
General Campus AP PP(48 Ports)

Server Room Subnet

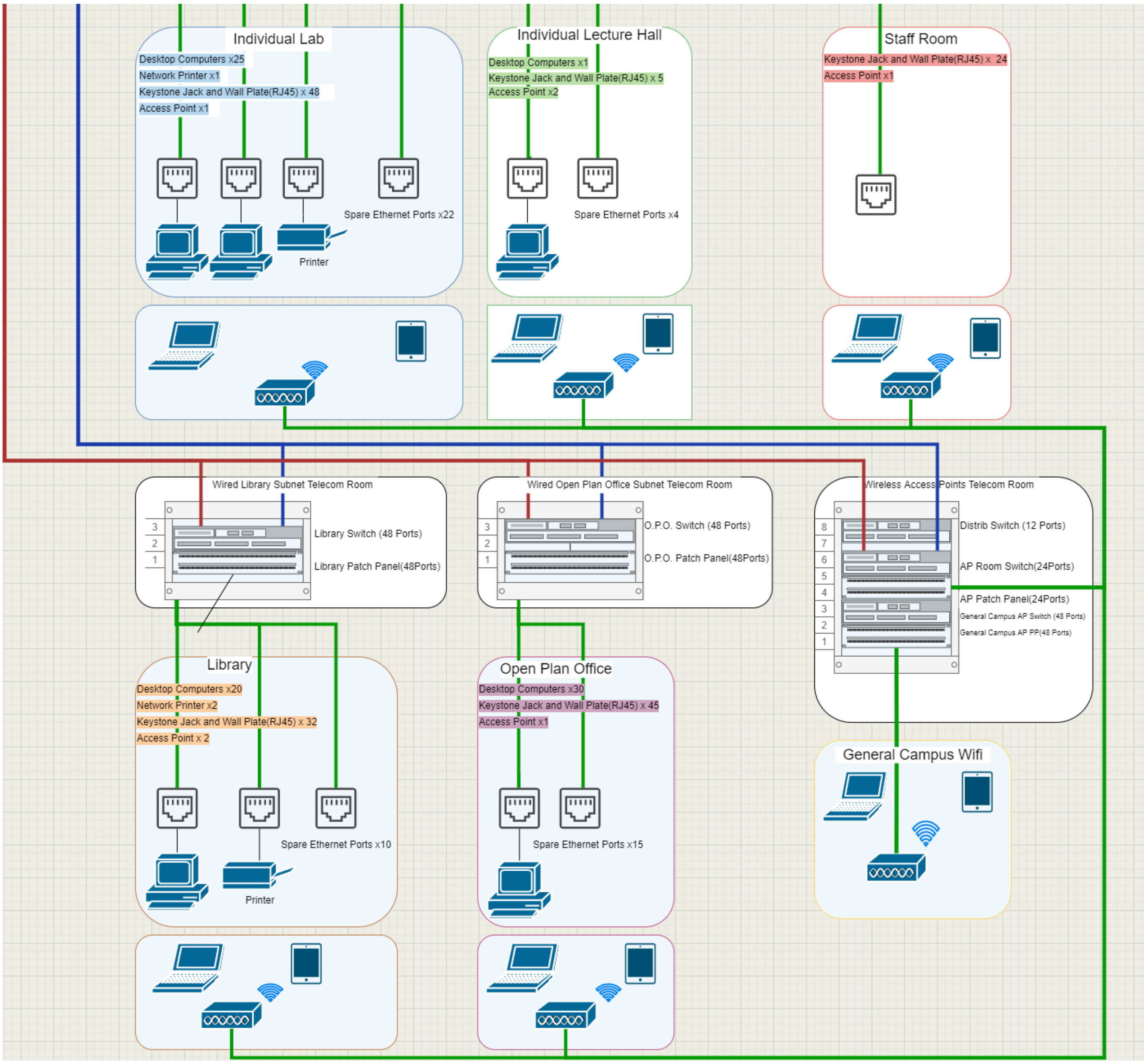
As discussed previously, the servers within the LAN will be on their own subnet, which depending on the choice of solution to use multiple virtual servers on a single machine or to use multiple physical devices, may necessitate more or less switching and patching ports within the racking unit.

Horizontal Cabling

The horizontal consists of repeaters, and Cat 6e twisted pair copper cables. As explained in the cabling section, the horizontal cabling is used to connect the telecoms rooms with their associated work areas. This 'work area' term is really a generalisation of groups of edge devices, such as APs and Desktop PCs. In the diagrams, horizontal cabling is represented by green lines.

Work Areas

The work areas as outlined above have been broken down into the following general layouts and facilities. Note that not only are minimum wall jacks provided for the wired work areas, but spares have been provided to account for expanding needs, such as additional desks/workspaces.

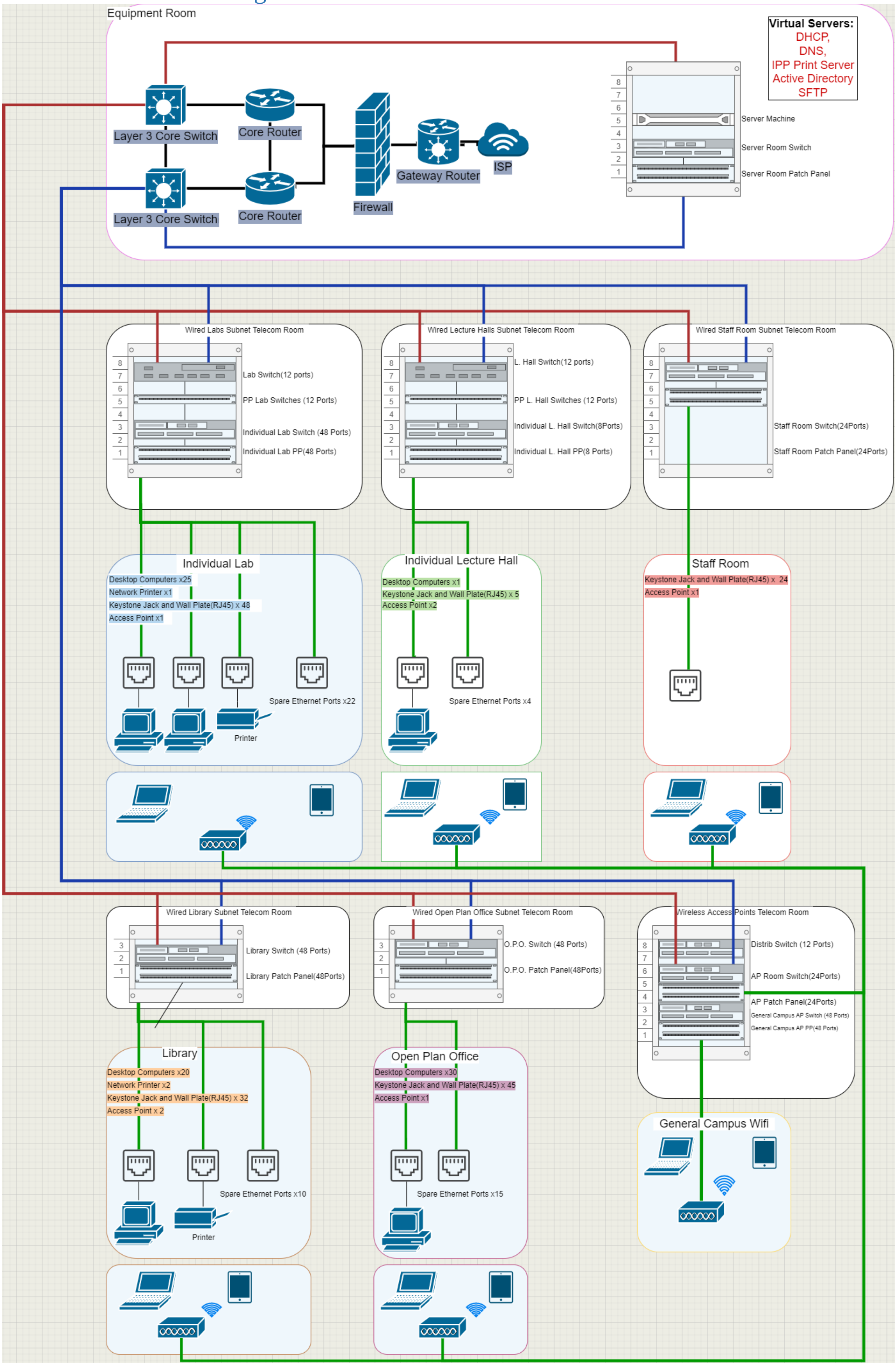

Individual Lab
Desktop Computers x25
Network Printer x1
Keystone Jack and Wall Plate(RJ45) x 48
Access Point x1
Spare Ethernet Ports x22
Printer
Individual Lecture Hall
Desktop Computers x1
Keystone Jack and Wall Plate(RJ45) x 5
Access Point x2
Spare Ethernet Ports x4
Staff Room
Keystone Jack and Wall Plate(RJ45) x 24
Access Point x1
Wired Library Subnet Telecom Room
Library Switch (48 Ports)
Library Patch Panel(48Ports)
Wired Open Plan Office Subnet Telecom Room
O.P.O. Switch (48 Ports)
O.P.O. Patch Panel(48Ports)
Wireless Access Points Telecom Room
Distrib Switch (12 Ports)
AP Room Switch(24Ports)
AP Patch Panel(24Ports)
General Campus AP Switch (48 Ports)
General Campus AP PP(48 Ports)
Library
Desktop Computers x20
Network Printer x2
Keystone Jack and Wall Plate(RJ45) x 32
Access Point x 2
Spare Ethernet Ports x10
Printer
Open Plan Office
Desktop Computers x30
Keystone Jack and Wall Plate(RJ45) x 45
Access Point x1
Spare Ethernet Ports x15
General Campus Wifi

General Security Concerns

Beyond the obvious requirement of a hardware Firewall on the outward facing portion of the LAN, and the inclusion of software Firewalls on fixed client devices such as the lab computers, it is important to address the security concerns that can arise from devices that can leave and re-enter the network, such as student/faculty mobile devices such as laptops, mobiles, and tablets. Of course, it is not possible to ensure that every person with multiple mobile devices install their own Firewalls, it is possible to limit the damage that such a breach may cause. The use of Multi-Layer ***managed*** switches provides an extra element of damage minimisation, as they allow for the deployment of VLANs (Virtual LAN) and afford monitoring and control of the network. The inclusion of a cloud-based or local Active Directory is also

(McCauley, 2019)

Full Network Diagram


Equipment Room
Virtual Servers:
DHCP,
DNS,
IPP Print Server
Active Directory
SFTP
Layer 3 Core Switch
Core Router
Layer 3 Core Switch
Core Router
Firewall
Gateway Router
ISP
Server Machine
Server Room Switch
Server Room Patch Panel
Wired Labs Subnet Telecom Room
Lab Switch(12 ports)
PP Lab Switches (12 Ports)
Individual Lab Switch (48 Ports)
Individual Lab PP(48 Ports)
Wired Lecture Halls Subnet Telecom Room
L. Hall Switch(12 ports)
PP L. Hall Switches (12 Ports)
Individual L. Hall Switch(8Ports)
Individual L. Hall PP(8 Ports)
Wired Staff Room Subnet Telecom Room
Staff Room Switch(24Ports)
Staff Room Patch Panel(24Ports)
Individual Lab
Desktop Computers x25
Network Printer x1
Keystone Jack and Wall Plate(RJ45) x 48
Access Point x1
Spare Ethernet Ports x22
Printer
Individual Lecture Hall
Desktop Computers x1
Keystone Jack and Wall Plate(RJ45) x 5
Access Point x2
Spare Ethernet Ports x4
Staff Room
Keystone Jack and Wall Plate(RJ45) x 24
Access Point x1
Wired Library Subnet Telecom Room
Library Switch (48 Ports)
Library Patch Panel(48Ports)
Wired Open Plan Office Subnet Telecom Room
O.P.O. Switch (48 Ports)
O.P.O. Patch Panel(48Ports)
Wireless Access Points Telecom Room
Distrib Switch (12 Ports)
AP Room Switch(24Ports)
AP Patch Panel(24Ports)
General Campus AP Switch (48 Ports)
General Campus AP PP(48 Ports)
Library
Desktop Computers x20
Network Printer x2
Keystone Jack and Wall Plate(RJ45) x 32
Access Point x 2
Spare Ethernet Ports x10
Printer
Open Plan Office
Desktop Computers x30
Keystone Jack and Wall Plate(RJ45) x 45
Access Point x1
Spare Ethernet Ports x15
General Campus Wifi
8
7
6
5
4
3
2
1

Chapter 4 – Operating Systems

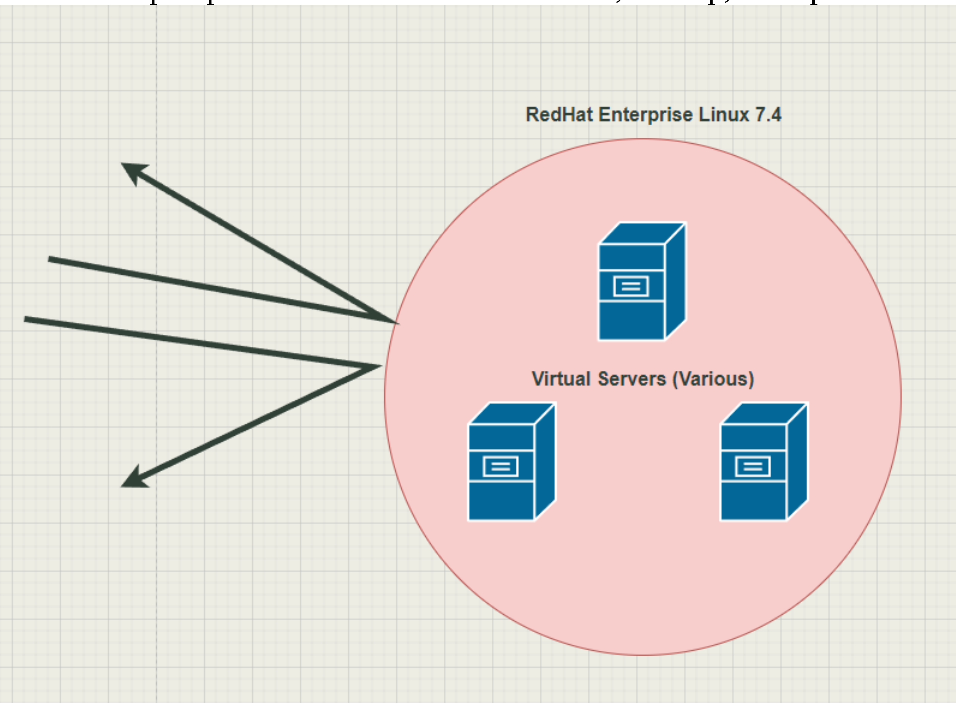
A crucial aspect in designing a network to provide services and functionality to its users is the operating systems that make up the machines on the network. This being so, there are a plethora of server and client operating systems available on the market that our LAN can make use of. While it may be useful to discuss various operating systems for client machines, due to compatibility, and their popularity among consumers, it makes sense to use Windows 10 for the client desktop machines on the network. Microsoft Windows currently boasts a whopping approximate of 80% of the market share for operating systems. This is partly due to the affordability of Windows machines compared to Mac, and their user friendliness when compared to Linux distributions. One of the major benefits of using a windows-based client, is that it allows for easier use of cloud-based services such as Microsoft Office 365, which can use browser-based and desktop applications for various services such as Microsoft Word, Excel, PowerPoint, and OneDrive. These are powerful and popular applications and the ability to integrate these services into client devices easily cannot be understated.

However, it is not so clear cut as to what operating system the server host machine will utilise. For this report it is understood that server machines will be utilised to host multiple virtual machines. The number of or purposes of the virtual server machines is not important to the discussion, but rather the choice of operating system that will be used for the host machine. The main two categories for consideration are between a Linux or a Windows Operating system. Listed below are major elements to consider between a Linux and a Windows machine.

	Windows	Linux
Ease of use	**Windows has a rich GUI and can be easily used by technical as well as non-technical persons. It is very simple and user-friendly.**	**It is mostly used by technical people because you should know various Linux commands to be able to work with Linux OS. For an average user, it will require significant time to learn Linux. Also, the troubleshooting process on Linux is complicated than on Windows.**
Installation	**Easy to set up. Requires far fewer user inputs during installation. However, it takes longer to install Windows as compared to Linux installation.**	**Complicated to set up. Requires a lot of user inputs for installation.**
Reliability	**Windows is less reliable than Linux. Over the recent years, Windows reliability has been improved a lot. However, it still has some system instabilities and security weaknesses because of its oversimplified design.**	**Highly reliable and secure. It has a deep-rooted emphasis on process management, system security, and uptime.**
Customization	**Windows has very limited customization options available.**	**Linux has many flavours or variety distributions which are highly customizable based on the user's requirements.**
Software	**Windows direct the greatest number of desktop users, and so the biggest selection of commercial software from third-party developers, many of which are not Linux compatible. It also leads in video games by a broad margin.**	**There are lots of software offered for Linux, and most of them are available as completely free and easy-to-install software packages. Additionally, various Windows programs can be executed on Linux with the help of compatibility layers for instance WINE. Linux is compatible with a broader range of free software than Windows.**
Support	**Both Linux and Windows offer extensive support. Windows 10 support is more easily accessible. If more extensive help is required, Microsoft offers support contract to its customers.**	**The best assistant is often found in peers, websites, and forums. Linux likely has an edge here due to the collaborative culture of open-source community. Some Linux companies like RedHat also do offer support contracts to customers.**
Update	**Windows update happens in the current moment which may be sometimes inconvenient to users. Takes more time to install and requires a reboot.**	**Users have full control when an update is made. Installation takes less time, and no reboot is required.**
Access	**Every user does not have access to the source code. Only the selected members of the group have access to the source code.**	**Users have access over the source code of kernel and can modify it accordingly. This gives a benefit that bugs in OS will be fixed faster. However, the drawback is that the developers may take undue advantage of the loophole.**
Privacy	**Windows collect all the user data.**	**Linux distros do not collect user data.**
Price	**Microsoft Windows typically costs between $99.00 and $199.00 USD for every single licensed copy. Windows 10 was offered as a free upgrade for existing Windows owners, however, the deadline for that offer has long since elapsed. Windows server 2016 data centre has a price starting at $6155.**	**Linux license remains completely free. However, organizations that need Linux support can choose for paid subscriptions for platforms like RedHat and SUSE. It's better to go with these subscriptions, otherwise, competent in-house Linux expertise can be expensive. Talking about the infrastructure cost, other things remaining equal (being on-premises or on the cloud), Linux being lightweight, we can expect 20% more throughput on Linux as compared to Windows.**

("Linux vs Windows Difference," n.d.)

The optimum choice for server host operating system is Red Hat Enterprise Linux (RHEL) 7.4, as not only is it supported by the previously selected server machine hardware, but it will also provide added security and less downtime to the network. While indeed difficult to configure, it should prove beneficial. Automated tasks can be set up to perform scheduled maintenance, backup, and updates of any virtual machines being hosted.



This being said, it does not imply that instances of Windows Server Machines will not be running. It must be considered how compatible the virtual servers will need to be with client devices, and other services. While possible, it is much more difficult to maintain Roaming User Profiles while using Active Directory on a Linux distribution. For the printer server, a RedHat Linux distribution can also be used. RHEL, Windows Server, and Windows all incur licensing fees for their use.

(“Server Operating System,” 2022)
(“Red Hat Enterprise Linux (RHEL) vs Windows Server,” n.d.)
(Davis, 2020)
(“Chapter 3. Installing Windows Virtual Machines Red Hat Virtualization 4.0,” n.d., p. 0)
(“Desktop Operating System Market Share Worldwide,” n.d.)
(JasonGerend, n.d.)
(“Linux vs Windows Difference,” n.d.)

Chapter 5 – Sub-netting Plan

The following section details the subnet plan for the LAN.

General Steps

- Identify the class. This will be A / B / C
- Identify the network and the node / host id.
- Apply the default subnet mask.
- Convert the default subnet mask to binary.
- Use the formula 2^n – 2 to determine the custom subnet mask (2 to the power of n minus 2)
- Determine the Least Significant Bit (LSB)

Implementation of Sub-Network

Required Subnets

- Labs

- Lecture Halls
- Library
- Staff Room
- Office
- Server Room
- Campus Wi-Fi

Identify the Class, and the Network and Node/Host ID

A standard class for a medium sized enterprise is a Class B Network. As such, the network ID can have a network ID of 172.16 to 172.31. Additionally, the default subnet mask for Class B is 255.255.0.0.

For our network 172.20 will be the network ID. For a class B the range in host addresses is 0.0 to 255.255. This is within the Private IP address range, so it is not routable to the outside world.

Network ID	Node/Host ID
172.16 - 172.31	0.0 - 255.255

Convert the Default Subnet Mask to Binary

IP Address	172	20	0	0
Default Subnet Mask	255	255	0	0
Default SM (Binary)	11111111	11111111	00000000	00000000

Determine Custom Subnet Mask

To identify the custom subnet mask, we use the formula $2^N - 2 = M$, where M is greater than or equal to the number of subnetworks needed. For this campus, we have 7 required subnets, as listed above, therefore M must be greater than 8. Using this formula, we see that N must, at minimum, be equal to 4. Seeing as $2^4 - 2 = 14$ we have and additional 7 subnetworks which can be used in the event that new facilities are required on the campus.

All bits within a subnet mask must be left-to-right contiguous. Therefore, we use our N from the previous equation as a number of 1's to add from left to right.

IP Address	172	20	0	0
Default Subnet Mask	255	255	0	0
Default SM (Binary)	11111111	11111111	00000000	00000000
CM (Binary)	11111111	11111111	11110000	00000000

Identify Least Significant Bit of Binary Custom Mask

In the binary CM, the least significant bit is the furthest right '1'. Taking this 1 and the rest of the 0's in its octal we get 1-0-0-0-0. With this number we convert back to decimal we get 16. This will act as the range of IP addresses available to each subnet.

("About Private IP Address Ranges," n.d.)
(Trost, 2009)
("Private Address Ranges," 2022)
("What is LAN (Local Area Network)?," n.d.)

IP Range (VLAN)	Host Address From	Host Address To	Broadcast Address
Labs	172.20.16.1	172.20.31.254	172.20.31.255
Lecture Hall	172.20.32.1	172.20.47.254	172.20.47.255

Library	172.20.48.1	172.20.63.254	172.20.63.255
Staff Room	172.20.64.1	172.20.79.254	172.20.79.255
Office	172.20.80.1	172.20.95.254	172.20.95.255
Campus Wi-Fi	172.20.96.1	172.20.111.254	172.20.111.255
Server Room	172.20.112.1	172.20.127.254	172.20.127.255

While in the table above the Server Room range is the similar to the other subnets, static IP addresses should be used for the servers that will be running on the LAN. This is so that client devices can reliably connect to them.
("When should I use a static or dynamic IP address?," n.d.)

Chapter 6 – Conclusion

This report has gone into great detail outlining the various components and services that are to be provisioned for this new college campus. Beginning with an outline of the brief requirements, the report then details the general guidelines for developing a LAN, the Network Components, Protocol and Services, and General Hardware that will be used throughout the facility. Within the Network Components, multiple product offerings for various devices are detailed and are selected for use within the LAN. The majority of which are Cisco brand products, with the exception of the access points, which are produced by Aruba. While discussing cabling, Structured Cabling System practices were researched, which was then used as a guideline for the implementation of the network.
The major components of the network are:

- Router (Gateway and Core): Cisco ISR 4461
- Core Switch: Cisco 9600 Series
- Hardware Firewall: Cisco Secure 3100
- Fibre Optic Transceiver (For Fibre Optic Backbone Cabling): Cisco FET-10G
- Distribution and Access Switches: Cisco 550x Series
- Access Point: Aruba 550 Series

For organization of network hardware, any standard racking unit can be used, alongside patch panels, cable ties, and other organizational tools.
General hardware, i.e., edge devices such as Desktop Computers, Servers Machines, and Network Printer Devices were also selected. These include the Dell OptiPlex XE4 for desktop machines running windows 10, the HPE ProLiant DL325 as a host server machine, and the HP Color LaserJet Enterprise MFP M681dh as the printer device.

The server machines will run on RHEL 7.4 and will host multiple different virtual servers to provide services to the network. These include DNS, DHCP, and print server, and may also include Active Directory, SFTP and other server types should cloud-based solutions not be pursued by the organization. For compatibility, Windows Servers may be used for the Active Directory and SFTP servers.

Following the research section, the actual network design was implemented. Using the components researched and structured cabling system guidelines, an abstracted network design layout was constructed. While the physical layout of the building was not available for this report, the abstracted network can be adapted to fit within those conditions. The network was separated into VLANs to provide additional security, these being logically organized by facility type. This is facilitated by the use of multi-layer managed switches.
The DHCP server will dynamically provide IP addresses using the subnet plan devised. A caveat is that the server subnet will not take part in this and will use static IP addresses for the servers on the network. This is to increase reliability for the client machines on the network.

References

About Private IP Address Ranges [WWW Document], n.d. URL https://community.helpsystems.com/kb-nav/kb-article/?id=5bf8247d-6bc3-eb11-bacc-000d3a1fe4c0&redirect=false (accessed 5.2.22).

Admin, 2018. What Is RJ45 SFP Module And How to Use It? Fiber Opt. Solut. URL https://www.fiber-optic-solutions.com/rj45-sfp-module.html (accessed 5.2.22).

Alice.Gui, 2015. Cat6 vs Fiber: What Is the Difference? Fiber Opt. Cabling Solut. URL https://www.cables-solutions.com/comparison-between-fiber-optic-and-cat-6-cabling.html (accessed 4.26.22).

AMD-EPYC-Data-Sheet.pdf, n.d.

Anonygoose, 2018. Answer to "Windows - How to allow clients to access their files across all machines connected to AD domain?" Serv. Fault.

Aruba 550 Series Wi-Fi 6 (802.11ax) Indoor Access Points [WWW Document], n.d. . Aruba. URL //www.arubanetworks.com/products/wireless/access-points/indoor-access-points/550-series/ (accessed 5.2.22).

Aruba Simplifies Enterprise IoT Adoption with New Automated Security and Next-Gen Wireless Solutions [WWW Document], 2019. URL https://www.hpe.com/us/en/newsroom/press-release/2019/04/aruba-simplifies-enterprise-iot-adoption-with-new-automated-security-and-next-gen-wireless-solutions.html (accessed 5.2.22).

Bhaumik, S., McGrath, A., n.d. Differences between OM1, OM2, OM3, OM4, OS1, OS2 fiber optic cable nomenclatures 3.

C9115AXI-EWC-X Price, Cisco C9115AXI-EWC-X GPL Price [WWW Document], n.d. URL https://ciscogpl.com/c9115axi-ewc-x.html (accessed 4.29.22).

Cat6 FTP Shielded PVC Solid Cable | Cat6 Cable [WWW Document], n.d. URL https://www.cablemonkey.ie/cat6-cable/13867-cat6-ftp-shielded-pvc-solid-core-cable.html#/56-length-305mt (accessed 4.25.22).

CATALYST 9600 Price, Cisco CATALYST 9600 GPL Price [WWW Document], n.d. URL https://ciscogpl.com/catalyst+9600.html (accessed 4.29.22).

Chai, W., Gillis, A.S., n.d. What is Active Directory (AD)? [WWW Document]. SearchWindowsServer. URL https://www.techtarget.com/searchwindowsserver/definition/Active-Directory (accessed 5.2.22).

Chapter 3. Installing Windows Virtual Machines Red Hat Virtualization 4.0 [WWW Document], n.d. . Red Hat Cust. Portal. URL https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.0/html/virtual_machine_management_guide/chap-installing_windows_virtual_machines (accessed 5.2.22).

Cisco 550X Series Stackable Managed Switches [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/products/switches/550x-series-stackable-managed-switches/index.html (accessed 4.29.22).

Cisco Catalyst 1000 Series Switches Data Sheet [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1000-series-switches/nb-06-cat1k-ser-switch-ds-cte-en.html (accessed 5.7.22).

Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Data Sheet [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741988.html (accessed 4.29.22).

Cisco Catalyst 9600 Series Switches [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/products/switches/catalyst-9600-series-switches/index.html (accessed 4.29.22).

Cisco Firepower 4100 Series Data Sheet [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html (accessed 5.2.22).

Cisco Secure Firewall 3100 Series - Cisco Secure Firewall 3100 Series [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/products/security/secure-firewall-3100-series/index.html (accessed 5.2.22).

Cohen, D.B., 2021. What Is NFS? Understanding the Network File System | Atera's Blog [WWW Document]. Atera - RMM Softw. PSA Remote Access MSPs. URL https://www.atera.com/blog/what-is-nfs-understanding-the-network-file-system/ (accessed 5.2.22).

Common Types of Network Cabling For Businesses | LeadingEdge, n.d. . LeadingEdge IT Serv. Solut. URL https://www.leadingedgetech.co.uk/it-services/it-consultancy-services/network-cabling/common-types-of-network-cabling-for-businesses/ (accessed 4.26.22).

Conrad, E., Misenar, S., Feldman, J., 2016. Chapter 5 - Domain 4: Communication and Network Security (Designing and Protecting Network Security), in: Conrad, E., Misenar, S., Feldman, J. (Eds.), CISSP Study Guide (Third Edition). Syngress, Boston, pp. 219–291. https://doi.org/10.1016/B978-0-12-802437-9.00005-9

Davis, H., 2020. Which is better Linux server or Windows Server? – QuickAdviser [WWW Document]. URL https://quick-adviser.com/which-is-better-linux-server-or-windows-server/ (accessed 5.2.22).

Desktop Operating System Market Share Worldwide [WWW Document], n.d. . StatCounter Glob. Stats. URL https://gs.statcounter.com/os-market-share/desktop/worldwide (accessed 5.2.22).

Ethernet Cables Explained | Tripp Lite [WWW Document], n.d. . Tripp Lite Website. URL https://www.tripplite.com/products/ethernet-cable-types (accessed 4.25.22).

Fisher, T., 2020. What Is DHCP? (Dynamic Host Configuration Protocol) [WWW Document]. Lifewire. URL https://www.lifewire.com/what-is-dhcp-2625848 (accessed 5.2.22).

Foley, M.J., 2021. Microsoft moves closer to running all of its own services on Azure | ZDNet [WWW Document]. URL https://www.zdnet.com/article/microsoft-moves-closer-to-running-all-of-its-own-services-on-azure/#:~:text=Five%20years%20ago%2C%20Microsoft%20still%20was%20not%20running,Live%20and%20Bing%20services%2C%20are%20running%20on%20Azure. (accessed 5.2.22).

Harmon, A., 2019. Understanding Firewall Tech Specs, Throughputs, & Datasheets. Firewalls.com. URL https://www.firewalls.com/blog/firewall-tech-specs/ (accessed 5.2.22).

Horowitz, M., 2022. Using VLANs for Network Isolation - RouterSecurity.org [WWW Document]. URL https://routersecurity.org/vlan.php (accessed 4.26.22).

Hot Standby Router Protocol Features and Functionality [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html (accessed 4.22.22).

How to: Assign 802.11b/g Access Point Channels [WWW Document], n.d. URL http://www.wireless-nets.com/resources/tutorials/assign_ap_channels.html#:~:text=Just%20ensure%20that%20all%20access,1%2C%206%20and%2011 (accessed 4.26.22).

How to Integrate Moodle LMS with Office 365?, n.d. URL https://www.o365cloudexperts.com/blog/moodle-lms-with-office-365 (accessed 5.2.22).

Howard, 2021. What Are the Different Types of Routers in Networking [WWW Document]. Blog. URL https://community.fs.com/blog/different-types-of-routers-in-networking.html (accessed 4.25.22).

HP® Color LaserJet Enterprise MFP M681dh (J8A10A#BGJ) [WWW Document], n.d. URL https://www.hp.com/us-en/shop/pdp/hp-color-laserjet-enterprise-mfp-m681dh#techSpecs (accessed 5.2.22).

HPE ProLiant DL325 Gen10 server | HPE Store US [WWW Document], n.d. URL https://buy.hpe.com/us/en/servers/proliant-dl-servers/proliant-dl300-servers/proliant-dl325-server/hpe-proliant-dl325-gen10-server/p/1010868976 (accessed 5.2.22).

HPE ProLiant DL325 Gen10 Server User Guide [WWW Document], n.d. URL https://techlibrary.hpe.com/docs/iss/dl325_gen10/setup_install/index.html (accessed 5.2.22).

HPE ProLiant MicroServer Gen10 x3421 Windows 10 Driver Support [WWW Document], 2020. . Hewlett Packard Enterp. Community. URL https://community.hpe.com/t5/Operating-System-Microsoft/HPE-ProLiant-MicroServer-Gen10-x3421-Windows-10-Driver-Support/td-p/7093522 (accessed 5.2.22).

Jake, 2019. NAS Performance: NFS vs. SMB vs. SSHFS [WWW Document]. Jake's Blog. URL https://blog.ja-ke.tech/2019/08/27/nas-performance-sshfs-nfs-smb.html (accessed 5.2.22).

JasonGerend, n.d. Deploy Network File System [WWW Document]. URL https://docs.microsoft.com/en-us/windows-server/storage/nfs/deploy-nfs (accessed 5.2.22a).

JasonGerend, n.d. Deploying Roaming User Profiles [WWW Document]. URL https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/deploy-roaming-user-profiles (accessed 5.2.22b).

Kath, H., 2020. SFTP and the Cloud: How to Transfer Your Data Securely [WWW Document]. www.goanywhere.com. URL https://www.goanywhere.com/blog/sftp-and-the-cloud-how-to-transfer-your-data-securely (accessed 5.2.22).

Kazmeyer, M., n.d. What Is the Purpose of a Firewall? [WWW Document]. Small Bus. - Chroncom. URL https://smallbusiness.chron.com/purpose-firewall-53858.html (accessed 5.2.22).

Keller, G., 2021. Can I Move Active Directory to the Cloud? JumpCloud. URL https://jumpcloud.com/blog/ad-to-the-cloud (accessed 5.2.22).

Kiran, 2021. Moodle™ vs MoodleCloud: Choose what's best for your e-learning site [WWW Document]. URL https://edwiser.org/blog/moodle-vs-moodlecloud-which-is-better-for-your-elearning-site/ (accessed 5.2.22).

Kirvan, P., 2021. What are the 6 components of structured cabling? [WWW Document]. SearchNetworking. URL https://www.techtarget.com/searchnetworking/answer/What-are-the-6-components-of-structured-cabling (accessed 4.26.22).

KwekuA, n.d. Set up multifactor authentication for users - Microsoft 365 admin [WWW Document]. URL https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication (accessed 5.2.22).

LAN, How to Set Up LAN Network? – Router Switch Blog, n.d. URL https://blog.router-switch.com/2012/02/lan-how-to-set-up-lan-network/ (accessed 5.2.22).

Lawrence Systems, 2020. Access Points and Creating WiFi VLANs Explained Using UniFi Wireless.

Layer 2 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x (Catalyst 9600 Switches) [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/16-11/configuration_guide/lyr2/b_1611_lyr2_9600_cg/configuring_spanning___tree_protocol.html (accessed 5.2.22).

Li, C., Lalani, F., n.d. The COVID-19 pandemic has changed education forever. This is how [WWW Document]. World Econ. Forum. URL https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/ (accessed 5.2.22).

Linux vs Windows Difference: Which Is The Best Operating System? [WWW Document], n.d. . Softw. Test. Help. URL https://www.softwaretestinghelp.com/linux-vs-windows/ (accessed 5.2.22).

List of printing protocols, 2022. . Wikipedia.

Liu, S., 2018. What Is Distribution Switch and Why Do We Need It? Medium. URL https://medium.com/@sylvieliu66/what-is-distribution-switch-and-why-do-we-need-it-c6978a8826b9 (accessed 4.22.22).

Lorenzo, 2015. How to enable Roaming Profiles on Windows Server 2012 R2 [WWW Document]. URL https://thesolving.com/server-room/how-to-enable-roaming-profiles-on-windows-server-2012-r2/#:~:text=Roaming%20Profiles%20allow%20users%20of%20an%20Active%20Directory,is%20how%20they%20are%20easy%20to%20set%20up. (accessed 5.2.22).

Loshin, P., n.d. What is Network File System (NFS)? [WWW Document]. SearchEnterpriseDesktop. URL https://www.techtarget.com/searchenterprisedesktop/definition/Network-File-System (accessed 5.2.22).

Lutkevich, B., n.d. What is an Edge Router? Definition from SearchNetworking [WWW Document]. SearchNetworking. URL https://www.techtarget.com/searchnetworking/definition/edge-router (accessed 5.2.22).

McCauley, G., 2019. Network Switch: Managed vs Unmanaged [WWW Document]. URL https://www.fieldengineer.com/blogs/network-switch-managed-vs-unmanaged (accessed 5.2.22).

Moris, M., 2021. Layer 2 vs Layer 3 Switch: Which One Do You Need? [WWW Document]. Blog. URL https://community.fs.com/blog/layer-2-switch-vs-layer-3-switch-which-one-do-you-need.html (accessed 4.25.22).

Moving away from a physical shared network drive [WWW Document], 2019. URL https://cloudmarket.com/news/moving-away-from-physical-drive/ (accessed 5.2.22).

Network File System (NFS), 2019. . GeeksforGeeks. URL https://www.geeksforgeeks.org/network-file-system-nfs/ (accessed 5.2.22).

NexGenT, 2017a. What is a VLAN? Virtual Local Area Networks.

NexGenT, 2017b. What is the Purpose of a Router?

Nganga, P., 2022. How to Find the Best Wireless Access Point [WWW Document]. Blog. URL https://community.fs.com/blog/what-is-wireless-access-point-and-how-to-choose.html (accessed 4.26.22).

Notenboom, L.A., 2013. Is My Router Acting as a DNS Server? Ask Leo. URL https://askleo.com/is-my-router-acting-as-a-dns-server/ (accessed 5.2.22).

Oliveira, iPLANiT-H.R. de, n.d. Print & Document Solutions [WWW Document]. URL https://www.datapac.com/services/print-document-solutions/ (accessed 5.2.22).

OptiPlex XE4 Small Form Factor PC : OptiPlex Computers | Dell Ireland [WWW Document], n.d. . Dell. URL https://www.dell.com/en-ie/work/shop/desktop-computers/optiplex-xe4-small-form-factor-build-your-own/spd/optiplex-xe4-sff/xctooxe4sff_vp (accessed 5.2.22).

Pedamkar, P., 2019. What is DHCP? | Understanding of Dynamic Host Configuration Protocol. EDUCBA. URL https://www.educba.com/what-is-dhcp/ (accessed 5.2.22).

Private Address Ranges [WWW Document], 2022. URL https://prod.ibmdocs-production-dal-6099123ce774e592a519d7c33db8265e-0000.us-south.containers.appdomain.cloud/docs/en/networkmanager/4.2.0?topic=translation-private-address-ranges (accessed 5.2.22).

Red Hat Enterprise Linux (RHEL) vs Windows Server [WWW Document], n.d. . TrustRadius. URL https://www.trustradius.com/compare-products/red-hat-enterprise-linux-rhel-vs-windows-server (accessed 5.2.22).

Roaming user profile, 2022. . Wikipedia.

Rubenking, N.J., 2022. How (and Why) to Change Your DNS Server [WWW Document]. PCMag UK. URL https://uk.pcmag.com/security/138870/how-and-why-to-change-your-dns-server (accessed 5.2.22).

Sarah Lewis, Burke, J., n.d. . IoT Agenda. URL https://www.techtarget.com/iotagenda/definition/gateway (accessed 4.25.22).

Schultz, D., 2022. Choosing the Right Termination - Keystone Jack vs RJ45 Connector vs Field Termination Plug [WWW Document]. trueCABLE. URL https://www.truecable.com/blogs/cable-academy/choosing-the-right-termination-keystone-jack-vs-rj45-connector-vs-field-termination-plug (accessed 4.26.22).

Sebastian, 2022. MoodleCloud. Moodle. URL https://moodle.com/solutions/moodlecloud/ (accessed 4.22.22).

Server Operating System: Server OS Types & How to Choose [WWW Document], 2022. . Knowl. Base PhoenixNAP. URL https://phoenixnap.com/kb/server-operating-system (accessed 5.2.22).

Server Rack Sizes: Understanding the Differences, 2020. . RackSolutions. URL https://www.racksolutions.com/news/blog/server-rack-sizes/ (accessed 4.26.22).

SFTP Server Active Directory | Tbsoftinc.com [WWW Document], n.d. URL https://www.tbsoftinc.com/sftp-server/set-up-active-directory-or-ldap-authentication-in-turboftp-file-transfer-server.html (accessed 5.2.22).

Star Network Topology [WWW Document], n.d. . https://www.conceptdraw.com. URL https://www.conceptdraw.com/How-To-Guide/star-network-topology (accessed 4.29.22).

Telecommunications Horizontal Cabling and Support Structure - UIT | Montana State University [WWW Document], n.d. URL https://www.montana.edu/uit/wiringguidelines/horiz-cabling-support-struct.html#:~:text=The%20horizontal%20cabling%20shall%20be,76%20meters%20(250%20feet) (accessed 4.26.22).

Top 11 Most Powerful Networking Companies Across Globe - [WWW Document], n.d. URL https://www.imedita.com/blog/11-most-powerful-networking-companies/#:~:text=Cisco%20holds%20the%20largest%20market%20share%20of%20almost,CISC

O%20certifications%20to%20students%20which%20are%20recognized%20worldwide. (accessed 4.29.22).

Trost, R., 2009. Chapter 1: Network Overview [WWW Document]. Netw. World. URL https://www.networkworld.com/article/2260776/chapter-1--network-overview.html (accessed 5.2.22).

Universal Networks [WWW Document], n.d. . Univers. Netw. URL https://www.universalnetworks.co.uk/ (accessed 4.26.22).

Wang, K., 2017. What Is the Crossover Cable? Medium. URL https://medium.com/@Katherine.WangFS/what-is-the-crossover-cable-ad5e74d980be (accessed 4.26.22).

What is a Hardware Firewall? [WWW Document], n.d. . Check Point Softw. URL https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-hardware-firewall/ (accessed 5.2.22).

What is a LAN? Local Area Network [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html (accessed 4.28.22).

What is Auto-MDIX feature in ethernet switches [WWW Document], n.d. URL https://www.omnisecu.com/basic-networking/what-is-auto-mdix.php (accessed 4.26.22).

What is DNS? DNS Explained [WWW Document], n.d. . NS1. URL https://ns1.com/resources/what-is-dns (accessed 5.2.22).

What is LAN (Local Area Network)? | DDI (Secure DNS, DHCP, IPAM), n.d. . Infoblox. URL https://www.infoblox.com/glossary/lan-local-area-network/ (accessed 5.2.22).

What is Network Topology? Best Guide to Types & Diagrams - DNSstuff [WWW Document], 2019. . Softw. Rev. Opin. Tips - DNSstuff. URL https://www.dnsstuff.com/what-is-network-topology (accessed 4.20.22).

What Is Optical Fiber Technology, and How Does It Work?, 2018. . NAI Group. URL https://www.nai-group.com/optical-fiber-technology-how-it-works/ (accessed 4.26.22).

What is Software Firewall? Difference between Hardware Firewall and Software Firewall [WWW Document], n.d. . SANGFOR. URL https://sangfor.com/blog/cybersecurity/what-is-software-firewall-difference-between-hardware-firewall-and-software-firewall (accessed 5.2.22).

What is the Difference Between Access Point and Router? [WWW Document], n.d. URL https://www.ligowave.com/difference-between-access-point-and-router (accessed 4.26.22).

What is VLAN? How VLAN Works and Common Examples [WWW Document], 2019. . N-Able. URL https://www.n-able.com/blog/what-are-vlans (accessed 4.22.22).

When should I use a static or dynamic IP address? | Ireland [WWW Document], n.d. . StarTech.com. URL https://www.startech.com/en-ie/faq/networking-general-static-or-dynamic-ip-address (accessed 5.2.22).

When to use a seperate DHCP server vs having router do DHCP? [WWW Document], n.d. . TechExams Community. URL https://community.infosecinstitute.com/discussion/91915/when-to-use-a-seperate-dhcp-server-vs-having-router-do-dhcp (accessed 5.2.22).

Why You Need Both a Hardware and Software Firewall [WWW Document], n.d. . SecurityMetrics. URL https://www.securitymetrics.com/blog/why-you-need-both-hardware-and-software-firewall (accessed 5.2.22).

Wide Area Networks (WAN) Considerations | PaperCut [WWW Document], n.d. URL https://www.papercut.com/kb/Main/WideAreaNetworkConsiderations#option-1-deploy-a-papercut-site-server (accessed 5.2.22).

Windows Internet Printing Service - IPP - RDR-IT, 2019. URL https://rdr-it.com/en/windows-internet-printing-service-ipp/ (accessed 5.2.22).

Wong, M., 2017. Core Switch & Edge Switch: How to Make a Decision? Medium. URL https://medium.com/@mikowong405/core-switch-edge-switch-how-to-make-a-decision-be4319e90216 (accessed 4.24.22).