**Report**

Contents

[IP Addressing and Network addressing scheme. 1](#_Toc512335679)

[LAN and VLAN 2](#_Toc512335680)

[Switching and Routing 2](#_Toc512335681)

[Ethernet 3](#_Toc512335682)

[DHCP 3](#_Toc512335683)

[HTTP 4](#_Toc512335684)

[DNS 4](#_Toc512335685)

[ACL 5](#_Toc512335686)

[Final info 5](#_Toc512335687)

[Reference list 6](#_Toc512335688)

There are many concepts within computer networking that may apply to this situation, including how to connect the two campuses together.

First, some assumptions.

Suppose the two buildings are of equal size such that the configuration for the two campuses are the same. Suppose also that each room has up to 60 computers within them.

# IP Addressing and Network addressing scheme.

With these two assumptions in place, one of the first tasks is to divide each building into networks and assign each an address. Like road names and house numbers can be used to deliver a parcel, a network address allows a computer to send and receive information. This is fundamental in allowing computers to be far more useful than they would otherwise be on their own.

I said that a room may have no more than 60 computers. This allows a subnet to be used with a mask of 255.255.255.192/26. This allows 62 hosts in that room so as few addresses are wasted as possible. If this changes in the future to need more (say 100 hosts) then a mask of /25 would be used, allowing up to 126 hosts. For your information, these addresses would be C type addresses.

Each room would have a unique address, for this you can use a convention like the following:

A B C D

100. 101. 55. 195

A – the first value can represent the campus. You can use an identifiable value here to dictate which building is used to allow addresses used in one campus to be used in the other.

B – the second value can dictate the floor that the room is on. In conjunction with the value in A, it becomes clearer where the machine is.

C – the third value can dictate the room the host is in. Room numbers may repeat on each floor, but each floor will only have one occurrence of the room number.

D – the last value can represent the machine number, as each host likely has a number associated already this would be simple to integrate.

Chapter 3 of J.D. Wegner and Robert Rockell (2000) “Private Addressing and Subnetting Large Networks” mentions the idea of using Private Addresses, allowing for the university to implement an addressing scheme that only needs to be unique within the buildings. “Such networks can still use private addresses and a technique called Network Address Translation (NAT) to convert those private (inside) addresses to public (outside) addresses.” This gives you flexibility over the addressing scheme chosen.

# LAN and VLAN

What use is an address if it is unreachable from other addresses? Both with building addresses and IP addresses, there needs to be some way to reach an address or there is no use for the place associated to the address.

Devices can be connected into Local Area Networks (LAN) to accommodate communication between the devices. J Law (2016) defines a LAN as “A network of computers and associated devices linked together within a limited area or a common environment, such as an office building.” This means that each campus can be referred to as a LAN, but collectively they would be a Wide Area Network (WAN) as the two campus LANs are connected over a Geographically Wide area.

LANs are useful for managing a network where all hosts have the same access to resources (Internet, office equipment, storage space, etc) however if a host needs different access to resources than other hosts, it can either be physically wired differently, or it can be separated into a separate Virtual Local Area Network (VLAN) to the rest of the hosts. A VLAN are LANs created by the switch, where the connection from one port is associated with another.

For the University, the Tutor machine in the room will likely have different permissions to that of the student machines. If all rooms have a switch, each tutor machine can connect to port 1. The port 1 of each room can be part of a tutor VLAN, treating each tutor machine differently to the student machines. An abstraction of Sripanidkulchai, K., Issariyapat, C., & Meesublak, K. (2008) mentions the power that VLAN give by allowing different machines to have different access rights regardless of the user.

# Switching and Routing

Data is sent in packets. Rather than creating a dedicated connection between hosts, which can be costly, these packets are sent to many different hosts to reach its destination. Once a packet reaches a router, the router will either forward it to another address, or discard the packet. This is switching. Like motorways connect parts of the country and have junctions that vehicles can use to get on and off, packets move from router to router until it can leave and reach its destination. In chapter 1.1.1 of Fall, K. & Stephens, R. (2011) many details about the concepts of switching, including the history of the dedicated phoneline, the usage of First in First out (FIFO) buffer management, etc. It details many of the deeper aspects of switching and TCP/IP in general.

As Switches connect devices to create networks and Routers connect networks, the functions of Routing are slightly different to that of Switching. Switching makes use of a Media Access Control (MAC) address, whereas Routing makes use of an Internet Protocol (IP) address. The MAC address is assigned by a manufacturers Network Interface Controller (NIC) and stored in Read Only Memory (ROM) and can’t change, while an IP can be assigned by a user in a static context or dynamically assigned by a DHCP server (Mentioned later in the report) from a list of available addresses.

These concepts are the backbone of contemporary communication over networks.

# Ethernet

One of the most common forms of wired data transmission globally, Ethernet is a constantly evolving form of data transmission. It first appeared in the 1970’s, meaning it has been very successful to last nearly 5 decades. Gigabit ethernet appeared in 1999 which was far faster than any other cable. With these faster speeds, network architecture changed from Bus topologies – one shared cable for all machines – to Star topologies. These star topologies have central switches and routers to connect the devices. To send packets over ethernet using TCP/IP, the data is split into packets. Then TCP segments and IP datagrams are added to the packet to make a TCP/IP packet. For Ethernet, more data specific to ethernet data transmission is used.

Because of the widespread utilization of Ethernet, there is lots of support for it, and there are lots of devices that cater to the use of Ethernet.

# DHCP

I have previously mentioned the use of DHCP for IP configuration. The power of DHCP is great, as it allows devices to be allocated an IP address automatically. This allows new devices to be quickly and easily added to the network. The server is configured to have a variety of available addresses, which the DHCP server can then forward data to when it receives a packet with that address on. In the case of the university, the addresses available would be that of all user machines (Not services like servers) as these addresses are able to change so long as they don’t need to be connected to by devices that require a static IP address. This would be used instead of the static addressing scheme (Although parts of that including building and floor can be) as the DHCP can’t prioritise an address for a specific host. The DHCP is able to provide address “lease-durations” where an address is allocated for a specific amount of time. There are many strategies that can be employed depending on your use of the system. Hall, E. (2000) makes the following suggestions:

“ The first calls for leases to be renewed halfway through a working day (such as having them expire every eight hours, which will cause them to be renewed after four hours). Another strategy is to set the lease duration to a multiple of two and a half times the working day (that is, 20 hours for an eight-hour working day), causing the leases to completely expire overnight and thus be renegotiated every morning. The former strategy works well on networks that keep their machines running all of the time, while the latter strategy works well on networks where systems are powered down or otherwise removed from the network at night.”

If you keep your machines on 24/7 then the first suggestion will be the best for you. It can renew during the day so that addresses are correct throughout the day and people can continue their work as normal. If the computers are turned off at night, then the second suggestion is better, as addresses are re-allocated at night so that the addresses are functional in the morning.

# HTTP

Likely one of the most famous acronyms within computing, the Hyper-Text Transfer Protocol (HTTP) is an internet protocol responsible for displaying information over the internet. When you search for a website, you receive information in the form of a HTTP packet with data written in Hypertext Markup Language (HTML). HTML is responsible for the actual data for a website, using tags (for example “<head>”, “<body>” etc.) to mark normal text as hypertext. Geeks for Geeks (2015) notes that, for the case of HTML “the HTML tags are used to help render web pages as well in the Browser” and HTTP “is a protocol for transferring the hypertext pages from Web Server to Web Browser.”

You will likely have a HTTP server on campus for the university website or for university web services. These would use HTTP to send and receive data from the server to the host machine, while the data itself would be written in HTML. What does this mean for you? The HTTP segment of the server is a software system that allows information exchange between the host and server, while the physical memory of the server holds the information for the website. The more information you need to store for the website, the more storage your HTTP server will require. You will likely want to use another storage device for some data, like usernames and passwords. This will help to protect data from malicious attacks and also reduce the quantity of data on the server. You will already have a server that allows people to access the host machines (I will refer to this as the Users server). It is possible to link this to the HTTP server such that the Users server treats a HTTP request the same as any other host from within the campus. This would allow an ACL (I will talk about this in more detail later) to be applied specifically to the HTTP requests such that some functions are not accessible via the internet, also helping to make the service more secure.

# DNS

The last type of server I will talk about. A Domain Name Server (DNS) is like an interpreter for people who use different languages. www.google.com is easier to remember than 8.8.8.8 (Bad example) as google is a name, or [www.hud.ac.uk](http://www.hud.ac.uk) being easier to remember than 161.112.232.60. These IP addresses are used by the servers and other components to send data packets between the servers and the hosts. However, just like programming languages, the computer doesn’t understand human language nor do humans understand machine code (easily). This can pose an issue. While programming languages use compilers and interpreters, browser requests use DNS servers. DNS servers have a long list of addresses along with their domain name (like www.google.com and www.hud.ac.uk). You can find the IP of a website in the command prompt of a windows machine by typing tracert followed by the domain name, E.G. tracert www.google.com (tutorial by thermoelectric (2008)) This may be useful for debugging in the future.

This is important as you would require a DNS, either on campus or provided by an internet service provider (ISP), to add your online functions to a DNS such that users are able to search for the website using a domain name and not an IP. The use of a DNS allows users to more easily access online resources, and allow your website to appear in search results on search pages such as Google and Bing.

# ACL

As mentioned within the HTTP section, an Access Control List (ACL) does what is says on the tin. It controls the access to a device using a list to allow or disallow certain services. These can include blocking PING requests, access to some pages or features or the workspace of other users. This is a standard way of adding extra security to the network, however using an ACL does increase the load on the router that it is applied to, as it does more work. The more rules or restrictions in place, the more this matters as there is a larger access list that needs to be checked. It works by looking at an inbound packet and finding the sender, the destination and the use. If it is a match for a disallowed request, the packet is dropped and the data lost, while if it is allowed then it is forwarded to the destination.

This is useful for you as students who learn about “Hacking” or other network bypasses or other things to do to a network may attempt to do this to your network or the networks of another uni. This also means that people from outside the uni may attempt to attack your network. A Denial of Service (DOS) attack can be prevented by limiting the speed of the connection to an external host, allowing service to other hosts to still be possible, or outright block hosts unless they are added to the ACL as an address that is allowed. Although this would increase workload at the start and end of the years as access rights change, it may be able to improve the integrity of your systems. However, unlike a DOS attack, a DDOS (Distributed Denial of Service) attack uses multiple sources to overwhelm a service. [Digital Attack Map](https://www.digitalattackmap.com/) (2013) gives information about the impact of these attacks, including that 1/3 of downtime is due to DDOS attacks. One way these are carried out is that it is flooded with requests. The impact can be reduced if the router(s) are rate limited, and if the ACL is able to recognise obvious sources of malicious attacks.

# Final info

These are just some of the ways you can set up your network to be running, efficient, and secure. There are many more techniques that can be applied which would aid with the running of the network, but I hope that these points mentioned show the potential that a strong network has for the users at Newnet University.

As technology improves, so does the reliance upon a strong network infrastructure and the need for futureproofing within it.

# Reference list

Digital Attack Map. (2013). What is a DDoS Attack?. Retrieved from https://www.digitalattackmap.com/understanding-ddos/.

*Fall, K. & Stephens, R. (2011).*TCP/IP Illustrated Volume 1

Geeks for Geeks. (2015). What’s difference between HTML and HTTP ?. Retrieved from https://www.geeksforgeeks.org/whats-difference-html-http/.

Hall, E. (2000). Unleashing the power of DHCP. pg. 93: ABI/INFORM Collection

Law, J. (2016). *A Dictionary of Accounting* (5th ed.). Oxford University: Oxford University Press.

Sripanidkulchai, K., Issariyapat, C., & Meesublak, K. (2008). Inference of network-wide VLAN usage in small enterprise networks. In INFOCOM Workshops 2008, Phoenix, AZ, USA, Retrieved from <https://ieeexplore-ieee-org.libaccess.hud.ac.uk/document/4544620/>.

thermoelectric (2008). FIND THE IP ADDRESS OF A WEBSITE USING COMMAND PROMPT. Retrieved from <http://www.instructables.com/id/Find-the-IP-address-of-a-website-using-command-pro/>.

Wegner, J.D. & Rockwell, R. (2000). *IP Addressing and Subnetting Including IPv6*