Communication Technologies

Assignment 2

Unit 10

George Hotten

Signal Theory

Representing Data Electronically

Bits
A bit is the most basic unit in computing. It represents one of two values: a 1 or a 0. Bits are used to make up data and instructions and is what is used when sending data to different components at a physical level.

Byte
A byte is a group of 8 bits used to make up data. Bytes can make up data such as numbers and letters. Bytes can then be grouped together to make kilobytes, megabytes, gigabytes and higher.

Segment
A segment is data from the application layer of the OSI model broken down into smaller parts and where the TCP header is added to the smaller parts.

Packet
A packet is an encapsulation of data from the transport layer with an added destination and source IP address.

Frame
A frame is an encapsulation of data from the network layer with an added destination and source MAC address.

Synchronous and asynchronous transmission
Synchronous transmission is where data is sent without any gap in transmission and is considered more reliable and efficient compared to asynchronous. The transmission is considered full duplex meaning data can be sent in both directions synchronously. Data is sent either as blocks or frames.

Asynchronous transmission is where data is sent with potential gaps in transmission. To combat the lack of synchronisation, start and stop bits are added to the start and end of data to show where the data begins and ends. The transmission is considered half duplex meaning data can only be sent in one direction at a time. Data is sent either as a byte or a character.

Error detection and correction
Error detection is the ability to detect errors in a data stream which can often be caused by interreference or faults during transmission. This is to ensure the integrity of the data and to ensure all data is received correctly.

Error correction is the ability to reinstate data which may have been altered by a fault in transmission back to its original state. To fix the data, the receiver can send a request back to the sender re-requesting the data or by not sending an acknowledgement, causing the sender to assume the data was not received and to resent it.

Bandwidth limitations and noise
Bandwidth is the amount of data which can be transmitted between devices within a specific timeframe. The lower amount of bandwidth, the longer it will take for data to be sent and received to and from devices.

Noise is energy interference that degrades the quality of a signal. If there is a high amount of noise, there will be a high number of errors causing data to need transmission. This can heavily slow down network speed.

Please Turn Over

Methods of Transmission

Coaxial

Coaxial cables are used be telecom and internet provide around the world to allow users to send a received data from the internet. Coaxial is a type of cable that has an inner conductor which is surrounded by a layer of insulation, further surrounded by an insulating outer jacket. Data is transmitted via electrical signals through the centre conductor.
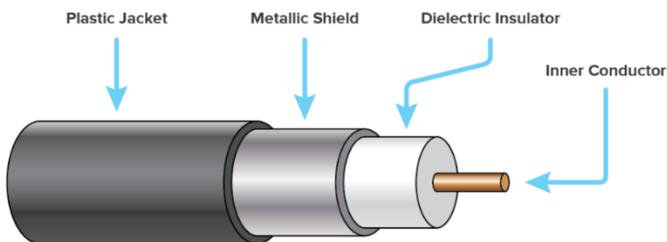
Optical Fibre

Optical fibre cables use thin strands of pure glass arranged in bundles. The strands of glass are very long and thin and are about the diameter of a human hair. This is called the core. Around the core is cladding which is outer optical material that reflects any light back into it. This is then surrounded by a buffer coating which protects the fibre from moisture and damage. Light is then sent through the cable to transmit data.
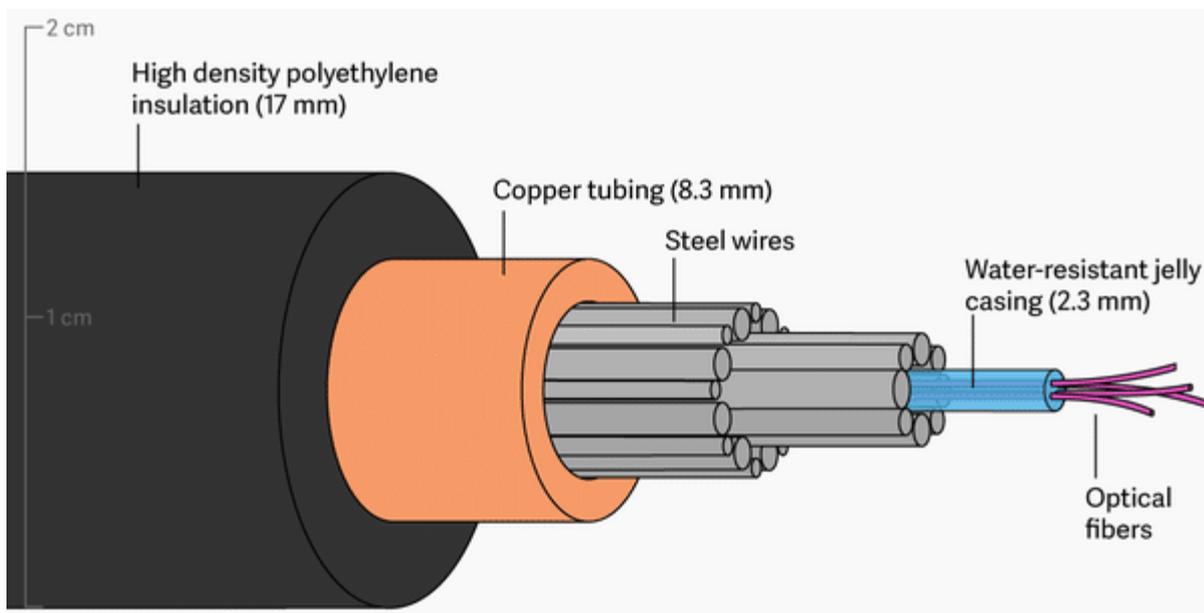
(Un)shielded Twisted Copper Pair

Twisted Copper Pairs describe how the wires inside the cable are laid out: twisted! The purpose of this is to help reduce interference. Compared to a coaxial cable, twisted pairs have multiple thin wires compared to coaxial single thick wire. To add further protection from interference, some twisted pairs have a shield around them to prevent any energy which may interfere with the signal.
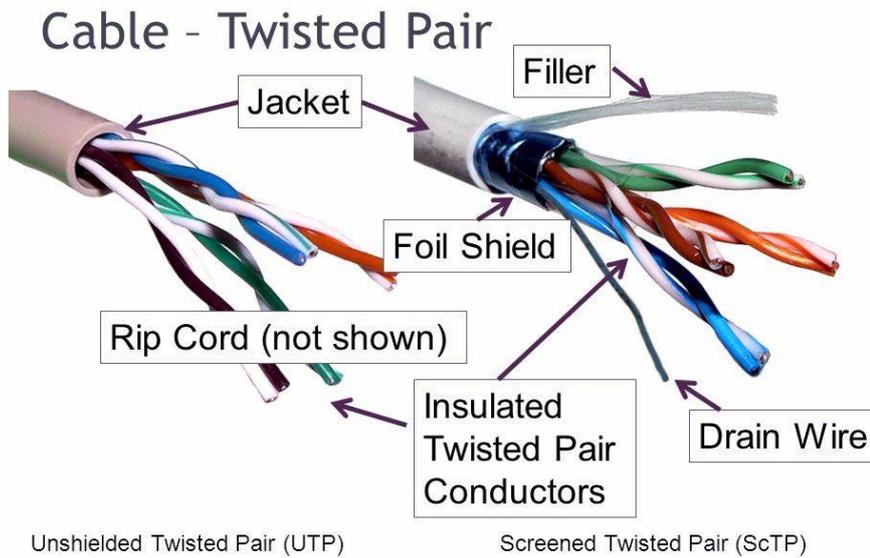
Radio

On radio, data is transmitted via radio waves using radio towers which can broadcast radio signals, in perfect conditions, almost halfway around the world. When a receiver picks up a radio signal, it is converted into a format the specific device can use, such as digital. Radio is used for many different systems, such as Wi-Fi and cellular.
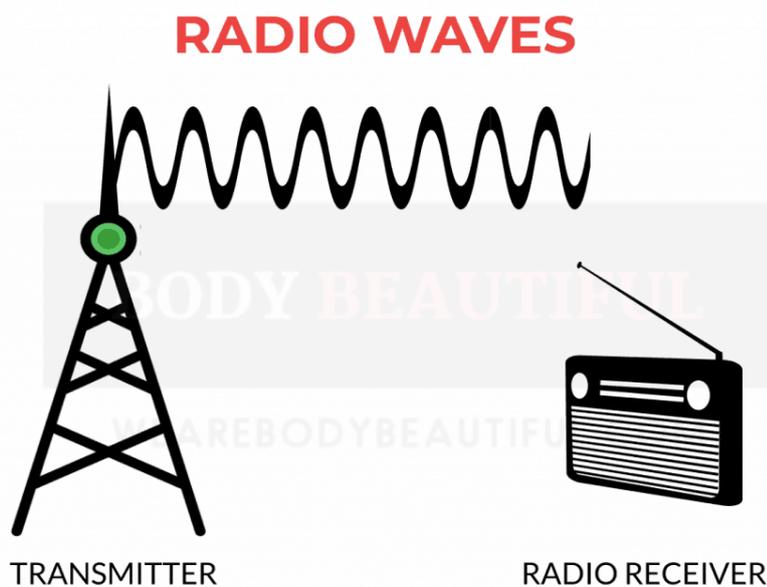
Satellite

On satellite, data is transmitted via radio waves using satellites which can be received by satellite dishes. This is mainly used for TV and communications from space. When wanting to communicate, data is sent up to a satellite, the satellites send data between each other so the data can be received in the correct area, and then the data is sent down in radio waves and is picked up by a satellite dish or receiver.
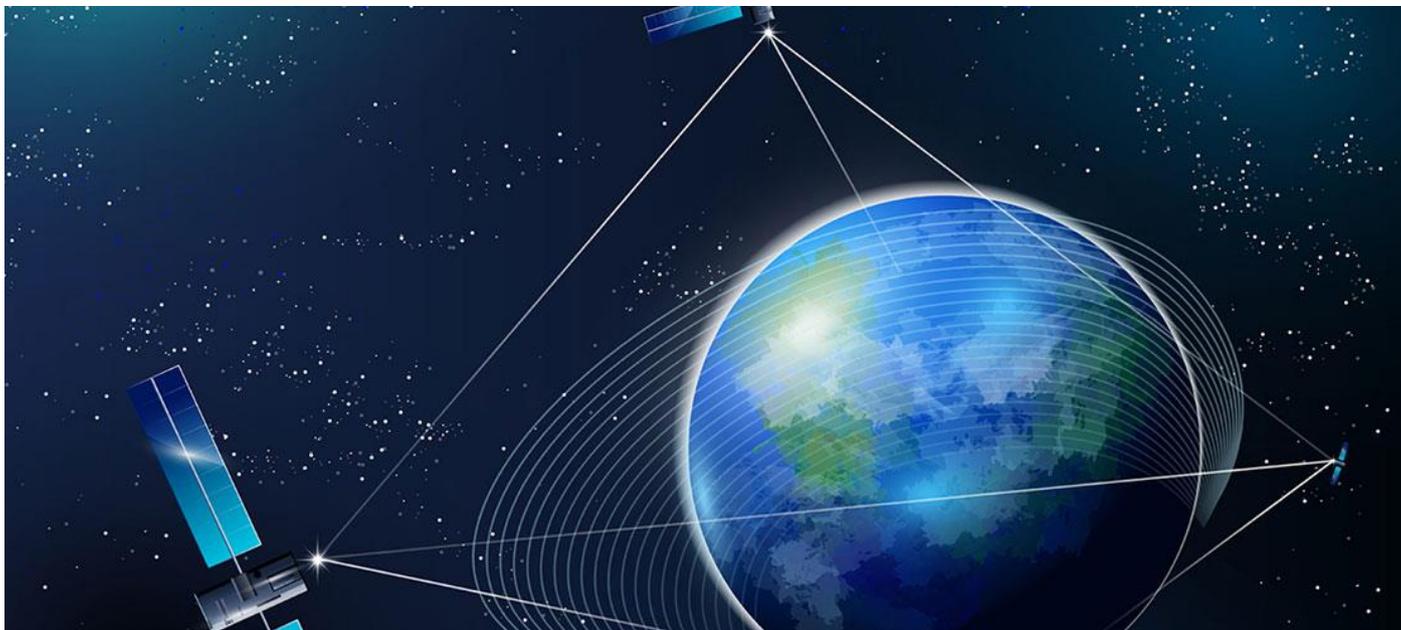
Where are the different transmission methods used?

Coaxial

Coaxial cables are mainly used for causes such as CCTV, (HD)TV and internet. These primarily use coaxial over the other methods as coaxial can support a longer cable length as they are better shielded. This makes it perfect for connecting to routers, watching CCTV or TV footage as the connection is faster than methods such as radio due to the connection being direct. This means you are more likely to get a better picture quality and a more reliable connection. Coaxial cables are relatively high speed too, making them suitable for larger sums of data that arrive with the internet and video streaming.

Optical Fibre

Optical Fibre cables are mainly used for the internet, networking, and medical research/procedures. These primarily use optical over the other methods as optical fibre is blazing fast as it uses light to sent data, which can provide over 10gbs of data per second. Optical fibre cables are especially used in surgery, especially procedures like an endoscopy whereas the cable is so small, it can reduce the size of the incision made making the surgery less invasive.

(Un)shielded Twisted Copper Pair

Twisted Copper Pairs are mainly used for gigabit LANs and phone networks. Compared to other methods, UTP and STP are affordable and provide good speeds for the average user. They are also protected from noise and interference by nature due to their twisted design, with some cables even having a protective shielding around them to make them even more resilient. Due to this shielding, they can be used over 100 meters, which is more than enough for small businesses and homes wanting to use a wired network. S/UTPs are mainly reliable and easy to replace if something goes wrong.

Radio

Radio is used mainly for long-range transmission of information, such as two-way voice and cellular/wireless networking. These primarily use radio rather than the other methods as radio signals do not require any cables to transmit data as it is all done through radio transmitters and receivers, meaning data can travel much faster and

father than if a cable was used. This allows for wireless networks such as Wi-Fi to function and is what cellular networks are built upon.

Satellite

Satellite communication is mainly used for television, internet, military applications, and emergency communication. These mainly use satellite over the other methods due to how far data can travel – up to 11 billion miles. This makes it most ideal for long-range communication to and from space, and for emergency situations where usual means of communication are down. Satellite also was most ideal for TV as the channels could be broadcasted almost anywhere in the world, with the only object the end-user required was a satellite dish to receive the signal.

Method Effectiveness

Transmission Method	Maximum Speed	Maximum Distance	Common Use
Coaxial	10mbs	500 meters	TV, HDTV, Internet, CCTV
Optical Fibre	10gbs	5000 meters	Internet, computer networking, research
UTP	Up to 10gbs depending on cable	100 meters	Gigabit Ethernet LANs or old telephone cable
STP	Up to 10gbs depending on cable	100 meters	Gigabit ethernet LANs
Radio	299,250 km/s	4 - 6 miles	Radio, TV, cellular
Satellite	506mbs	11 billion miles	Emergency communication, Communication with services in space

Wired and Wireless Networks

Transfer Rate

A wired connection uses cables such as optical fibre to send data between two devices, whereas Wi-Fi uses radio waves. A wired connection can hit around 10gb a second whereas Wi-Fi can hit a theoretical maximum of 6.9gb a second. However, 6.9gbs can only be hit in the most ideal conditions as Wi-Fi tends to be as slow as 1gb a second due to interference with walls and other devices.

The Effectiveness of Data Transfer

Wired networks are considered more stable and reliable as they are less disrupted by the environment around them, such as overlapping Wi-Fi signals and do not need to penetrate surfaces as they are a direct connection. Wired networks have much higher speeds too due to the direct connection, and depending on the cable used, use the speed of light to transmit data. Wired networks further have better security than wireless networks too as data being sent around the network cannot be sniffed as it is sent directly to and from the recipient, where as Wi-Fi broadcasts data out to all devices.

Wireless networks also have their perks. Data can be transmitted from anywhere where there is a signal and devices are free to move around the area as they are not constrained to a cable. Depending on the strength of the signal, data can be transmitted at around 6.9gbs, which isn't far off wired's 10gbs.

Ease of Use

Whilst a wired connection is typically faster, it is a lot harder to setup. This is because you need to have your home/business wired for ethernet which can be very expensive. It would also require the implementation of a switchboard, switch, and most cases, a dedicated cabinet room. Wi-Fi, on the contrast, only needs a wireless router or WAP to function. Once one is connected, it will broadcast its signal any device that is capable of joining will be able to connect without any major issues.

Distance

The capable distance of a network depends on its infrastructure. For example, a wired network using optical fibre could have data traveling up to around 5000 meters. However, Wi-Fi can be more complicated as it replies heavily on what WAP you use, the area the WAP is located and the speed of data transfer. The wireless signal can be easily disrupted by objects such as walls and floors. This can be further degraded by the band being used (such as 2.4Mz or 5 MHz) as the shorter the wave (the higher the MHz), the shorter the distance the signal can travel, making it more prone to materials it needs to penetrate.

Conclusion

To conclude, if security and reliability are your concerns, a wired network is perfect for you. As this setup uses cables, the connection to other machines is more direct meaning data is only sent where it is needed, and as the connection is direct the reliability of the data arriving correctly is drastically increased. Speed can also be an important factor, and if you need reliable speeds higher than a 1gb per second (which is plenty for most people), a wired network is your option.

However, if cost and ease of use are your concerns, go with a wireless network. Wireless networks can be up and running within minutes and don't require any extra hardware other than your router/wap combo. Speeds tend to be fast enough for the average user and the user isn't constrained by a cable, meaning they can be anywhere within the WAP's area (which most of the time is an entire modest size house!) without any drastic signal loss.

Practical: direction communication between two devices

Part One: The Direct Connection

I was tasked with setting up a direction connection between two devices. In my setup, all devices were connected to a switch board. To start with, I noted down the number of my computer, and the number of my peer's computer. C22 and C13.

I then went to the switchboard and plugged an ethernet cable from my port to my peer's port. The cable used is marked in red.
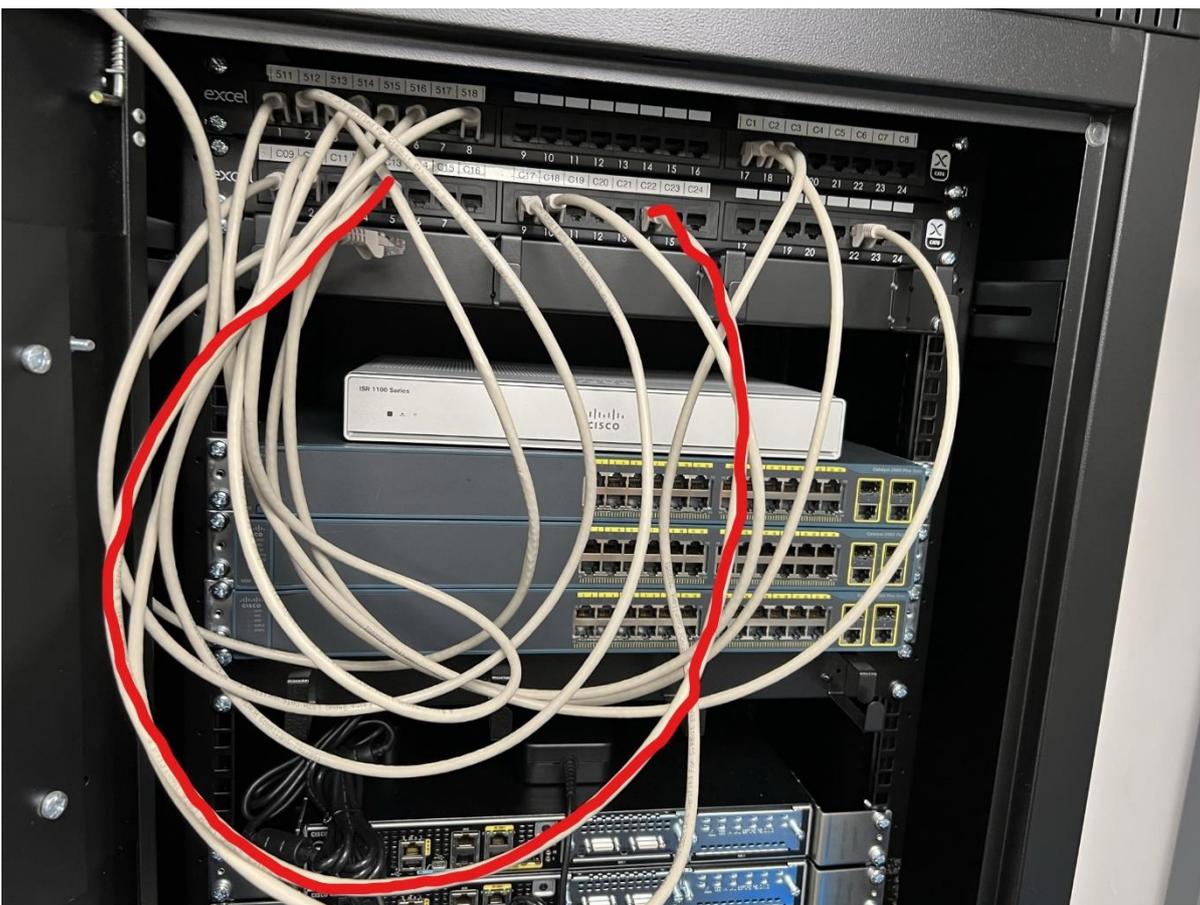
After that me and my peer configured our machines to use a Class A private IP address on the 255.0.0.0 subnet.
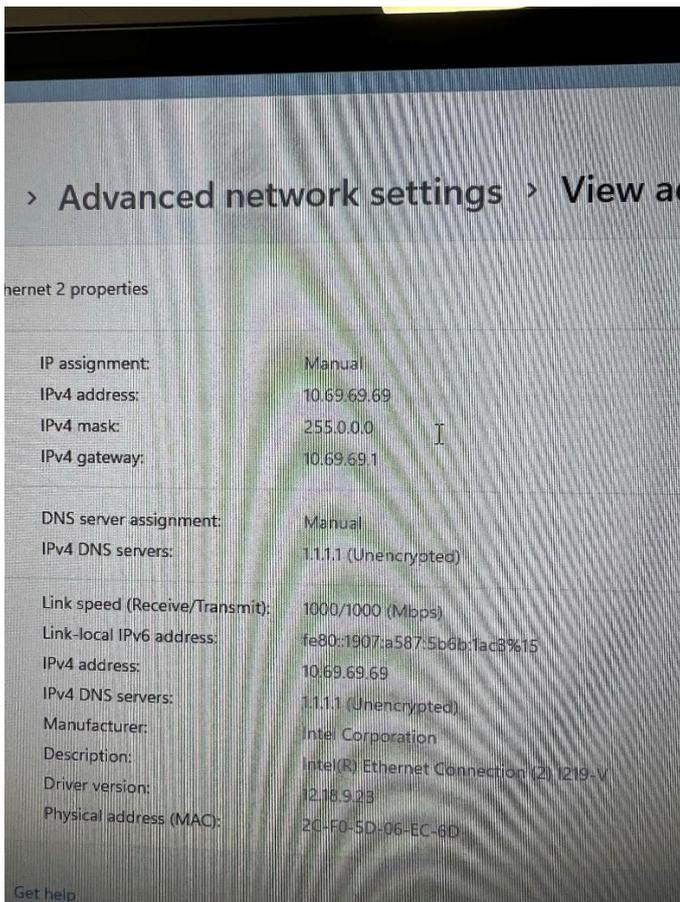
I used the IP address 10.69.69.69, whilst my peer used 10.69.69.80. From my machine, I attempted to ping my peer's IP address and I was successful, showing we created a direction connection.
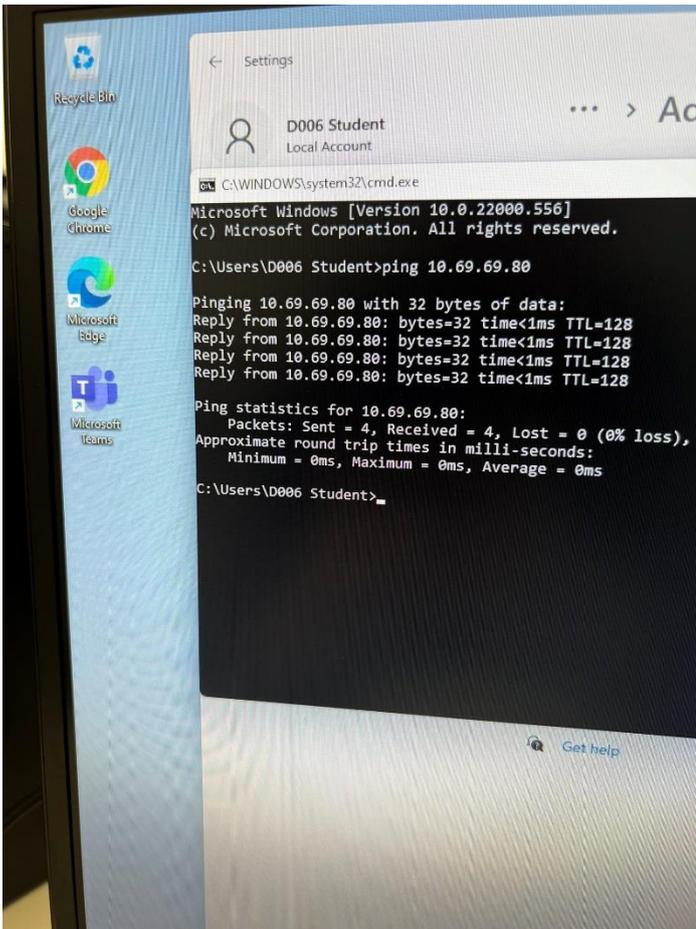
Part Two: Adding an Intercommunication Device

Following from part one, I was further tasked to add an interconnection device to the network. I chose to use a router. Before continuing, me and my peer switched our devices to be on different subnets. I kept my IP address of 10.69.69.69 on the 255.0.0.0 subnet whilst my peer switched to the Class C IP 192.168.69.69 on the 255.255.255.0 subnet. We also both configured our default gateways to the appropriate address, which we decided on being 10.69.69.1 and 192.168.69.1.

To start off, I turned on the router and plugged an ethernet cable from the router's G0/0/0 port into the C22 port on the switchboard (my machine, outlined in pink) and an ethernet cable from the router's G0/0/1 port into the C13 port on the switchboard (my peer's machine, outlined in red).
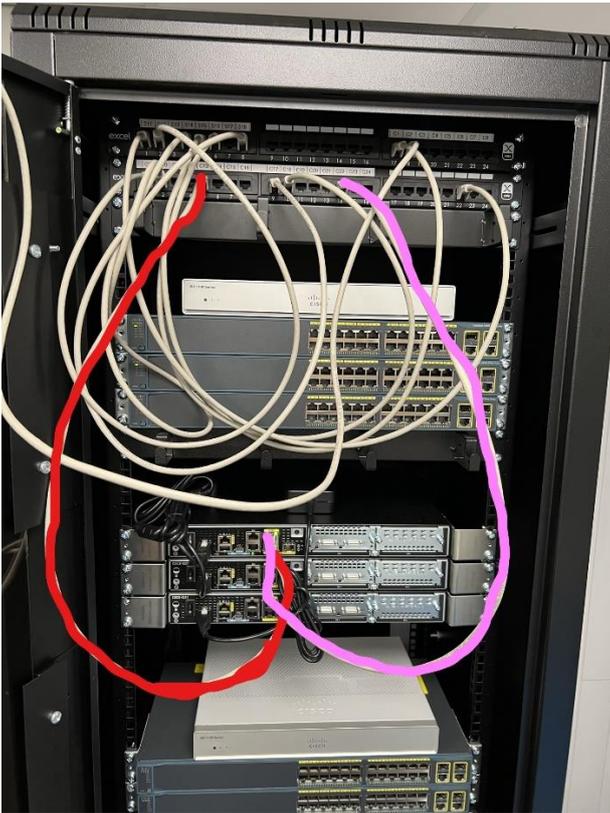
Now our devices are connected to the router, it is time to configure it. I started off by plugging into the router's serial configuration port and connecting that to my laptop. Here I can configure the IP address of the router and its subnet on each port. This is done using the following commands:

- en – enable the command line
- configure terminal – enter the configuration terminal
- interface G0/0/x – configure a specific interface (port)
- ip address y z – configure the ip address for that interface, Y being the IP and Z being the subnet
- no shutdown – enables the interface

This was repeated twice for both our interfaces.
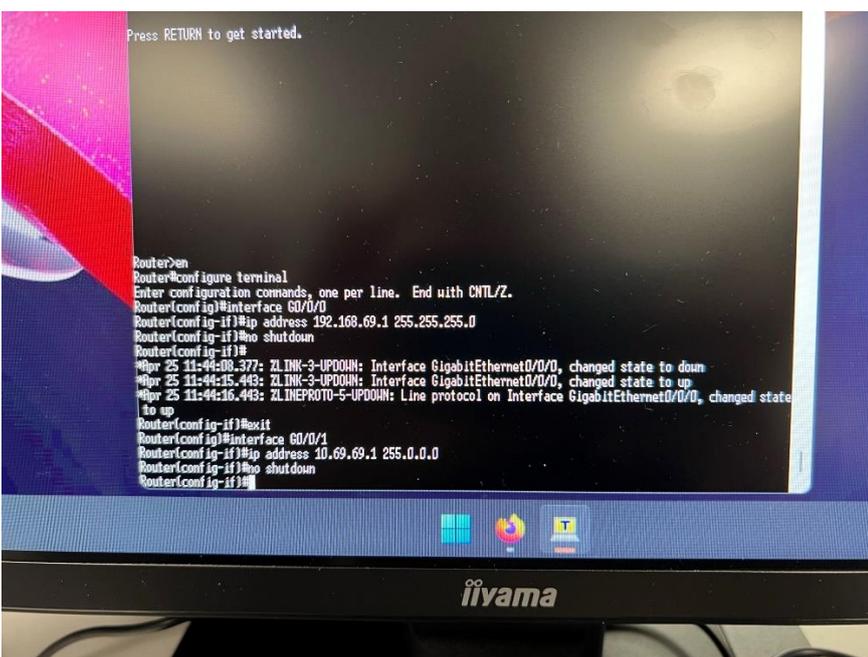
Now our router has been properly configured, we can go back to our machines and attempt to ping each other. I tried pinging 192.168.69.69 from my machine and was successful showing I had successfully added an interconnection device to my network.