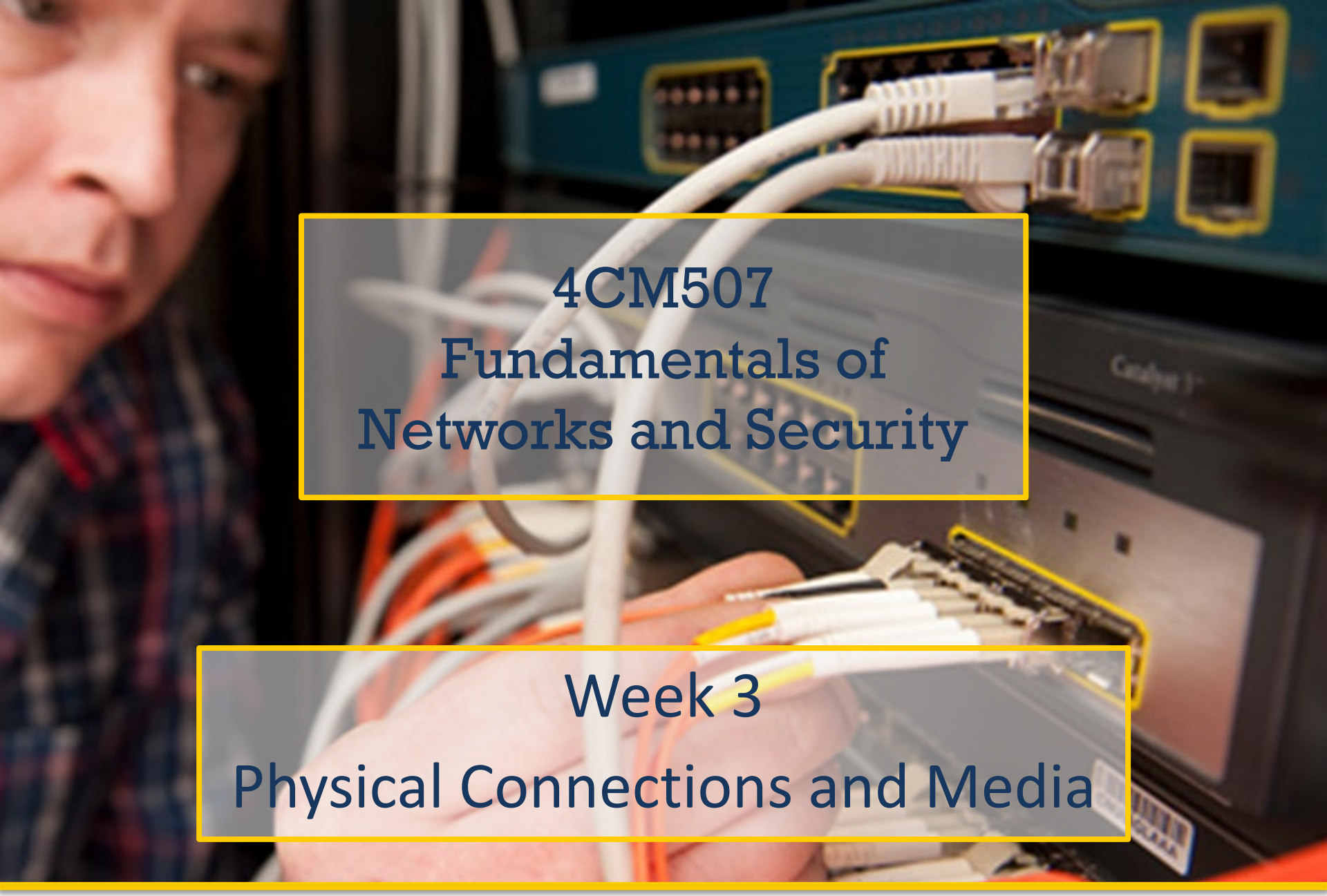


4CM507 Fundamentals of Networks and Security

Week 3
Physical Connections and Media

IMPORTANT INFO!!

- BE AWARE - YOU ARE BEING RECORDED

  This is part of the normal lecture process, recordings will be made available to you to support your studies

  Inform me as soon as possible if you object to recordings being made (and remind me every session!!)

- DID YOU TAP-IN?? DO IT NOW!

Week 3: Objectives

- Connection media
  - Fibre
  - Copper
  - Wireless
- LAN Equipment
- Inter-LAN Equipment
- Network Types
  - LAN / WAN / WLAN / MAN / PAN / SAN

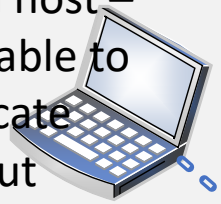
Recap…

- Last week we talked about the physical components found in networks
- The week before we found that networks are just clouds of things inside clouds of clouds

- This week we are looking at some of the ways that the Physical Components connect together to form the clouds

Some terminal stuff on the Local Area Network

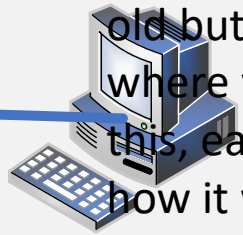
A mystical host – strangely able to communicate but without wires



A printer – churns out our stuff even if we are not connected directly to it – how does it know?

Something must be happening in here !

A PC - it might be old but you know where you are with this, easy to see how it works, just plug it in.

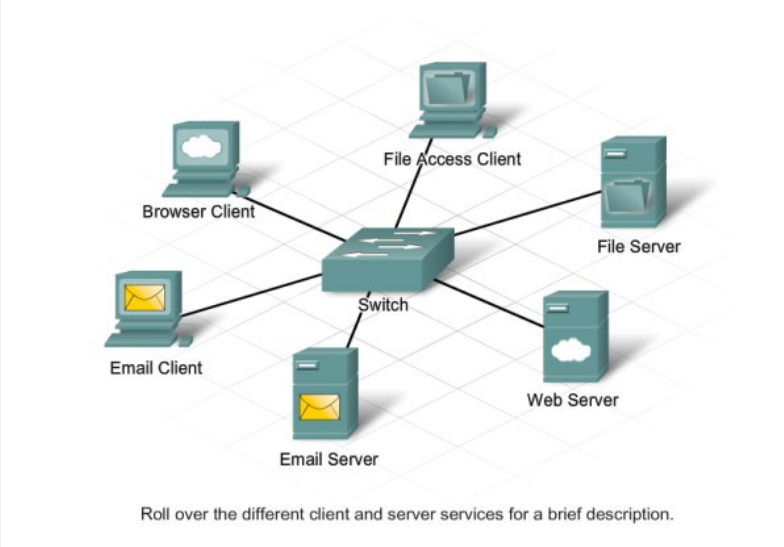


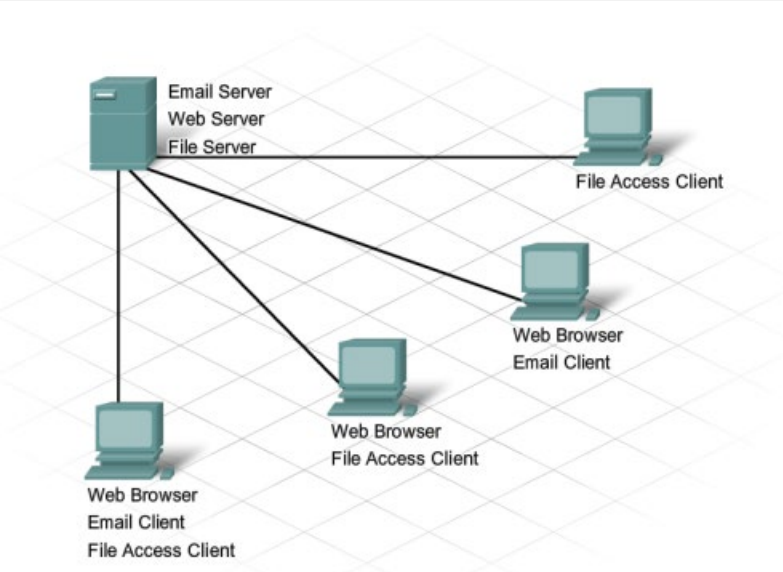
Server- how does it work? no screen, no keyboard but it knows everything – if we can hack this we can take down the world!

Looks like a book but … Too weird for words

Client – Server networks

- Clients - hosts with software that requests and / or displays information obtained from a server
- Servers - hosts configured with software to provide services and information to other (client) hosts on the network
- Servers can provide single or multiple services:





Connection and Connection Media

- In networks, what we need to do is get data to and from our devices
- Ideally as fast as possible and *probably* as reliably as possible (only probably???)
- What's the fastest thing that we know???
  - A Networks student at 13:55 on Monday?
- Light !!! That's the one! 186,000 miles (300,000,000 metres) per second
  - Marginally quicker than a lecturer at lunchtime!

Sending Data / Messages

- For many living things the most common and universal system is “gesticulating”
- Visible messaging usually sent over very short distances with a hope that the recipient is able to *interpret* the intended meaning
- Formal language is much harder, but quickly becomes necessary

- Out of interest, who identifies “thumbs up” as a positive gesture, who finds it offensive?

Make messages visible

- Interpreting Gesticulations can be a problem, over any distance it usually ***is*** a problem
- We need something more distinct and not open to interpretation
  - Smoke Signals?
    - Does that actually work?
  - Semaphore (flag waving)?
    - Good while you can make out body shapes
  - Morse code?
    - Can be seen over a much greater distance when using light

Make messages visible

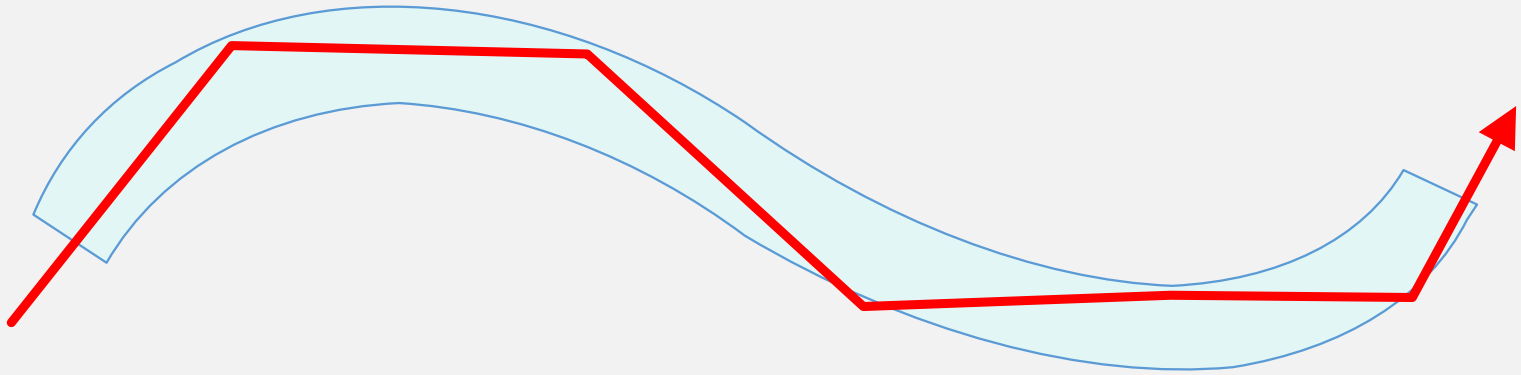
- You can see light from a long way but it has problems:
  - We need to change the messages to light
  - Light doesn't go around corners
  - We only see it on or off (like binary)
    - two flags at angles cannot be seen as far away
  - Everyone else can see it as well, it isn't private
    - We will talk more about security problems later, for now we will just say that messages can easily be intercepted and fabricated

Shine a Light!

- Changing electrical data signals from our CPU into some form of light is an expensive process in terms of power and time delay
- We need to turn the light on and off jolly fast but it takes time for the light to come on and go off again
  - LEDs do not light up until there is a certain voltage level, there is a “dead-band” where nothing happens
- To speed up the process we do not quite turn the light off (but that’s a story for another day…)

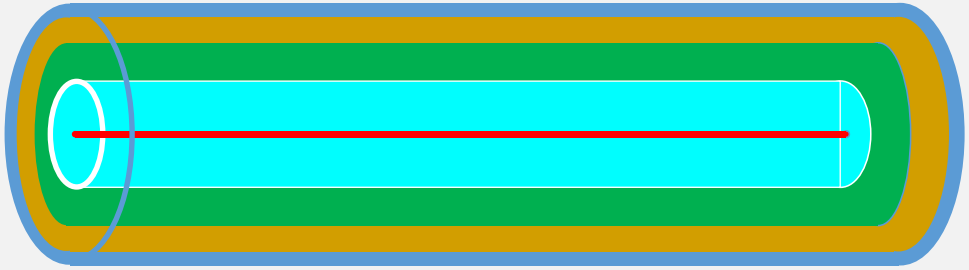
Fix the other problems

- Put the light in a tube
  - Hides the light from prying eyes
- Make the tube reflective inside
  - Light bounces round corners!

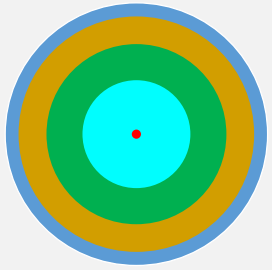


Fibre Optics – the "light tube"

- Difficult to make mirrors in tubes
- We see reflections on water because water has a different "refractive index" – optical fibres rely on this principle



Strengthening
Cladding
Core
Coating
Cover



Monomode fibre

- Driven by an expensive Laser (like the one that they do eye surgery with but less controlled)
- Very pure light, single wavelength
  - remember that white light is made from many colours, many wavelengths
- Very Long distance, high bandwidth
- Expensive to buy (including the lasers – one at each end)
- Expensive to install – very fine core, hard to terminate
- Fragile, easily broken
- DANGER! Will blind you if you look into it (not joking)

Multimode fibre

- Driven by a less expensive lower power Lasers or LEDs (like the led pointers that we like to use)
- Not such pure light, multiple similar wavelengths
  - e.g. dark red, very red, light red, a smidge orangey
- Long distance, high bandwidth
- Relatively expensive to buy and install
  - But not as expensive as monomode
- Hard to terminate
- Fragile, easily broken
- Lower energy, might not blind you, but why take the risk?

Copper cables

- Coax, very old tech. Different coax types RG62 (mainframe), RG58 (two way Radio, LAN, Virgin media?), RG59 (TV) are common (ish)
  - rare, very rare in LANs now, would not be installed

Copper cables

- Twisted pairs. Many types, often listed with “CAT” (category) numbers
  - Common in networks and many other applications

- Usually 4 pairs of twisted wire, twisted together
- We send signals as a voltage difference between a pair of conductors
  - The “difference” part is very important, it isolates the “ground reference voltage”

Some radio stuff

- Any single piece of wire acts like an aerial, it can be used to transmit or receive signals
- PVC insulation has minimal impact on this capability
- If we have the right equipment, we could measure the voltage collected by the length of the wire, amplify it and you can easily be listening to Radio 4 (where later today there will be an interesting discussion on herbaceous borders)

Some radio stuff

- Two separate wires near each other may pick up different signals or the same signals but at different times
  - Radio Frequency (RF) signals travel through space at roughly the speed of light, fast but not instantaneous.
  - There will be a time difference between a signal hitting one wire and then the other
- The “difference signals” will sometimes have a similar electrical characteristics as our data but they will not make sense - they will interfere with and corrupt the real data

Twisted pair cables

- If we twist the two insulated wires together they become very close, less time difference between pickup
- Along its length, each wire of the “twisted pair” will be alternately closer to and further away from the interfering signal
- Hopefully over a given time period, each wire of the “twisted pair” picks up the same signal at the same time

Twisted pair cables

- Twisting the signal pair together has the general effect of significantly reducing the Radio Frequency Interference (RFI) and Electro Magnetic Interference (EMI)
- If the same interfering signal is picked up by both wires in the pair, the interfering voltage goes up and down on both wires simultaneously meaning the voltage *difference* due to Electro Magnetic Interference (EMI) will be zero – it cancels out.
  - This is highly effective but nothing is ever perfect!

Twisted pair cables

- Extending this concept, the twisted pairs are then twisted together (Gigabit ethernet sends multiple bits at once and uses the difference between two pairs)
- The problems of EMI and crosstalk get worse as the cables become longer and as the data rate increases
- New “CAT” versions are usually aimed at reducing the problems
  - Cat5 had more “twists per inch” than cat3
  - Cat6a introduced “screening” or “shielding” as standard
- Be careful that some “standards” are not actually “standards” (yet or ever)

Wireless

- For wireless devices, the medium is electromagnetic waves through space
  - We often say “through the air” but EM waves do not need actual air otherwise you would not be able to watch Sky TV !

- There are benefits to wireless such as ease of connection, but it does have quite a few problems with being publicly observable (those cyber security problems again) and being affected by RFI and EMI

Wireless

- There are many wireless standards, using different frequencies, different bit transmission rates, …
- 2.4GHz is a common “carrier frequency” (About the same frequency as a microwave oven uses to cook food) (really)
- 5GHz is also common as a carrier
- You cannot use a 2.4GHz device on a 5GHz network (and vice versa) but it is now common for devices to have both capabilities
- 6GHz was introduced many years ago, it was ignored for sometime but is now popular again

Network Infrastructure Devices

- Following on from wires and connections, we need to consider devices that define the network
- Referred to as “Intermediary devices”
- Manage Data as it passes through the network
- Determines the path that messages should take based on destination host addresses (where the information is being sent to)

Network Infrastructure Devices

- Examples of intermediary network devices
- Network Access Devices (switches and wireless access points)
  - Often referred to as “Layer 2”
  - The wireless part of Wireless Access Points (WAP or AP) are actually Layer 1 not Layer 2 but we are not losing any sleep over this because we do not yet know what it means!
- Internetworking Devices (routers)
  - Referred to as “Layer 3”
  - Wireless Routers are Layer 3, Layer 1 and possibly Layer 2
- Security Devices (firewalls)
  - Often layer 3, 4 or even upper layers

Network layers

- Don’t worry, you haven’t missed anything!
- We will get back to these soon enough
- For this week you just need to know that these intermediary devices work in different ways and perform different functions, **they are not interchangeable**

Wireless Access Point, Wireless Router

- There are two main types of wireless network devices in IP networks that do different things, they are not interchangeable (though a WR contains AP)
- WAP or AP connects wireless clients to the local network
  - Makes this cloud accessible for wired and wireless clients
- WR connect clients to another network
  - Connects this cloud to another cloud
  - The WR at home connects your local network to the ISP/ Internet, only the home network is wireless (normally)

LAN equipment

- Layer 2 Switches (Commonly just called “Switches”)
- This is the “Really Clever” referred to in Week 1
- Data comes in from an “End device”, the “Really Clever” looks at the data then forwards it to a specific exit port based on the MAC address of the device physically connected to the exit port

A word on ports

- The word “port” is used to mean more than one thing in networking
- We have physical ports on a switch, the physical holes that we connect to. Switches normally have ports in multiples of 4 or 8 (4, 8, 12, 24, 48 are very common)
- We also have logical ports, these are a communication identifier. Some of these are “well known” or “registered” e.g. WWW is port 80.
- Logical ports can be any number between 1 and 65535
  - Google IANA if you want to know right now, or wait a few weeks!

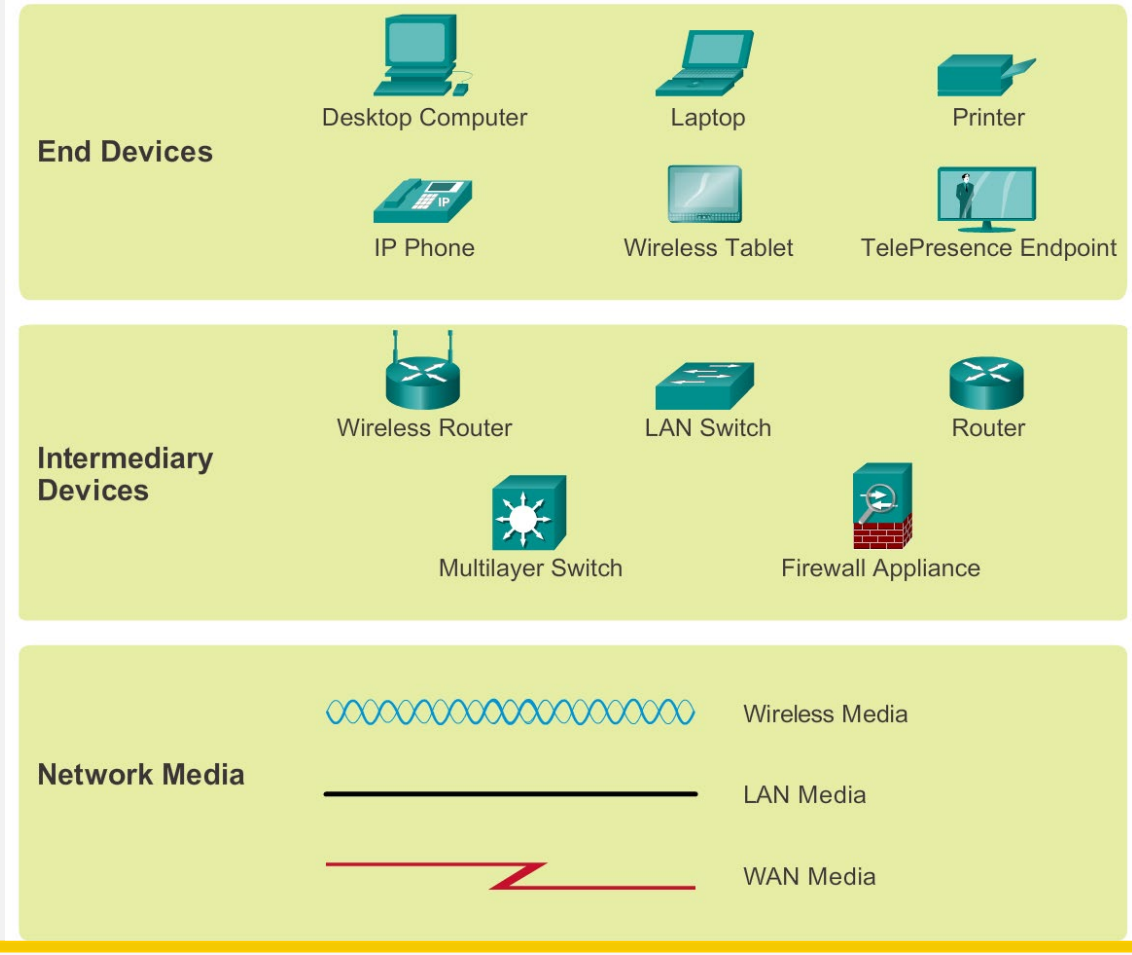
Inter-LAN equipment

- Most commonly discussed is the Router
- Most commonly deployed in enterprise networks is the Layer 3 Switch or Multilayer Switch
- This is the “Amazingly Clever” referred to in Week 1

Inter-LAN equipment

- A typical Router is likely to have between 2 and 4 physical ports (connect 2 – 4 LAN clouds together)
  - ISP routers may have may more ports but at a much higher cost
- It will be capable of translating between protocols such as adsl / cable broadband and ethernet/wireless LAN
- A typical Layer3 switch will only have ethernet ports but could provide routing for a different network connected to each one (12 – 24 clouds?)
  - Ethernet ports can be fibre or copper

Common Network Symbols

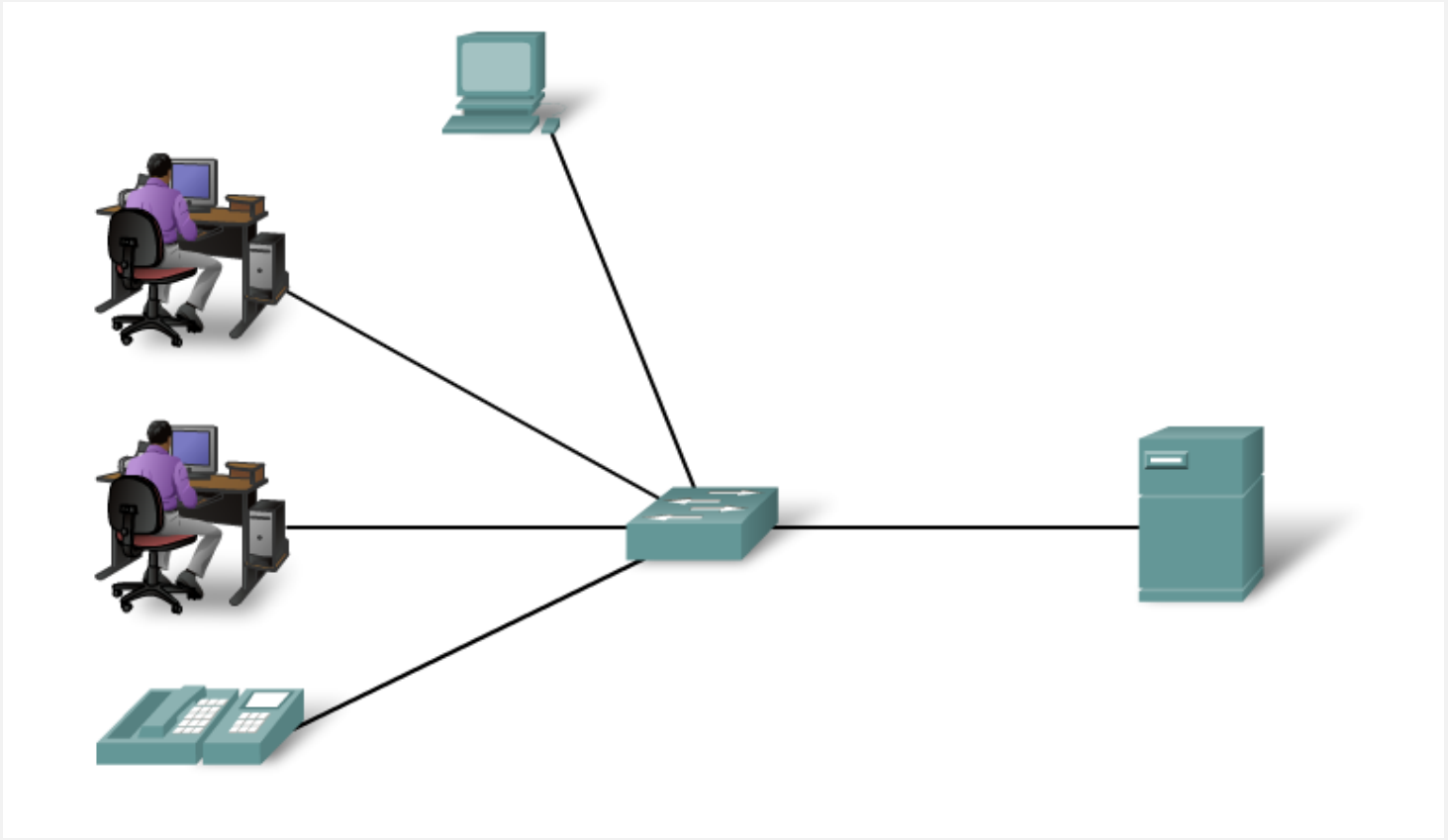


Types of Networks – what is in the cloud!

- Three common types of network infrastructures are:
  - Local Area Network (LAN)
  - Wide Area Network (WAN).
  - Wireless LAN (WLAN)

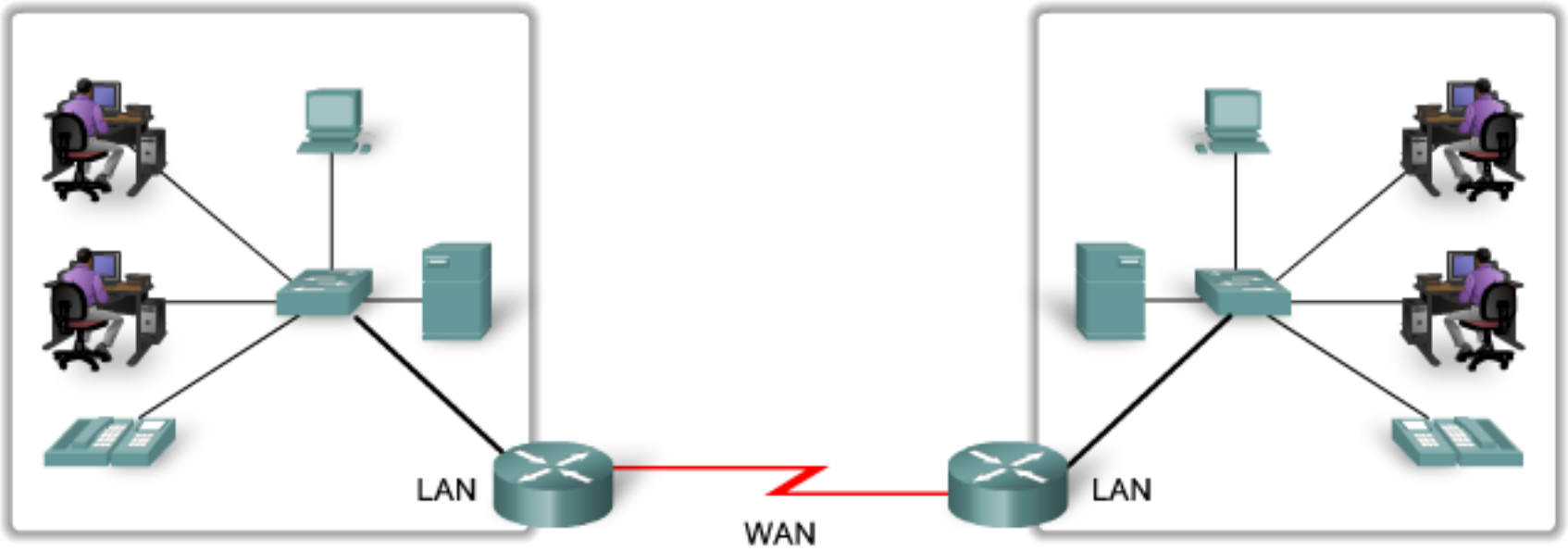
- Other types of networks include:
  - Metropolitan Area Network (MAN)
  - Personal Area Network (PAN)
  - Storage Area Network (SAN)
  - Wireless Internet / Wireless Broadband / “5G”

Local Area Networks (LAN)



Wide Area Networks (WAN)

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



Data Centers – jfi !

- A data center is a facility used to house computer systems and associated components including:
- Redundant data communications connections
- High-speed virtual servers (sometimes referred to as server farms or server clusters)
- Redundant storage systems (typically uses SAN technology)
- Redundant or backup power supplies
- Environmental controls (e.g., air conditioning, fire suppression)
- Security devices

Summary

- Connection media
  - Fibre
  - Copper
  - Wireless
- LAN Equipment
- Inter-LAN Equipment
- Network Types
  - LAN / WAN / WLAN / MAN / PAN / SAN

Email : j.hardy@derby.ac.uk
visit : MS310
phone : 01332 591732