Late 1960s internet developed as a project by the US department of defence.

* Began with ARPANET project
* www invented by tim berners lee in 1989
  + consists of webpages websites and hyperlinks
  + html was the language used for creating these webpages
  + http was the protocol for transferring web data
  + difference between www and internet is internet is more of a global structure while www was more of a network of all the webpages
* 1971 first email was sent
* 2000’s social media and broadband were on the rise
* 2010s – mobile internet, streaming services
* 2020s – 5g networks, IoT, AI

Physical structure

* Consists of data centres, fibre optic cables, submarine cables – under the oceans, carry most of the internet traffic, satellites, and wireless networks
* Backbone of internet – refers to the high capacity network of optical fibres and routers that form the core of the internet

Internet service providers

* Companies that provide users with access to the internet
* E.g Vodafone, Skynet
* Tier 1s own global backbone networks, tier 2 buy wan bandwidth from tier 1s and resell it, there is a tier 3 too.

WANs and LANs

WAN – wide area network – rely on third party carriers and connection therefore large geographical area, high latency since larger area and also therefore more insecure

LAN – local area network – cover small geographical area but faster (lower latency) often seen in small organisations such as schools

Topologies:

* Bus topology – a multipoint communication. All devices are connected to a single central cable.
* Star topology – each device has a dedicated point to point link only though a central node, which is typically a switch or a router
* Bus vs star
  + Bus – all devices share a central cable
  + Star – all devices are connected to a central node
  + Bus - data travels along the bus, all devices receive it, but the unintended computers will ignore it, but this causes security issue since it can be intercepted or stolen since it is sent to every device
  + Star – data is sent to the central node, which forwards it to the intended device
  + Bus – failure of the main cable affects whole circuit
  + Star – failure of one device will not affect another device since everything done through central node
  + Bus – slower due to data collisions, when collisions occur, the two computer attempting to transmit data wait a random amount of time before resubmitting, since if they collide the data corrupts, so that if they wait a random amount of time, they are less likely to collide, unless very unlikely, the random is exactly the same, this repeats.
  + Star – faster as each device is linked to the central node instead of through each other

Physical topology and logical

* Physical – actual physical layout of devices, cables, and connections in a network
* Logical – how data logically flows between devices on the network
* A network can have a different physical and logical topology
* In a star, if a hub is used instead of switch, it just redirects data to every device on network until it finds the right one, which makes it act like a bus effectively, hence outdated and hub is no longer used. Switch instead knows how to directly direct the data to the very intended computer without going through each one.

Wifi

* Allows devices connect to internet and communicate
* Developed by IEEE (institute of electrical and electronics engineers)
* Generations – IEEE standards:
  + 802.11 - 1997
  + 802.11b - 1999
  + 802.11a - 1999
  + 802.11g - 2003
  + 802.11n – wifi 4 - 2009
  + 802.11ac – wifi 5 - 2013
  + 802.11ax – wifi 6 - 2021
  + 802.11ax – wifi 6e – 2021
  + 802.11be – wifi7 - 2024
  + 802.11bn – wifi 8 – 2028 – not out yet
* Frequencies – higher frequency – faster, lower frequency – slower
* Higher frequencies are for shorter range and are less penetrating and experience less interference
* Lower frequencies are for longer ranges since more penetrating and longer range, but higher interference
* Wireless access point – wap is a device that allows wireless devices to connect to a wired network using wi fi,
* Wireless network adapter – hardware that connects to a main device#
* Network interface card – hardware component that enables a computer or device

MAC address

* Is a 48 bit hexadecimal number assigned to each device connected to the network

Mesh network topologies

* Full mesh network topology – every node connected to all other nodes
* Total number of connections is n(n-2)/2
* Expensive due to large number of links required
* Provides a high level of redundancy, data can take many paths to reach destinations, so if one link fails, it can just go a different path
* Partial mesh – every node is connected only to some other nodes
* More practical to implement than full mesh, providing balance between cost, redundancy and efficiency
* In most cases, important devices have more connections, less important have fewer connections
  + Partial is cheaper since fewer cables and equipment, less redundancy and easier to set up, less secure, less efficient, more congestion
  + Full mesh is more expensive since all devices connected to each other, but maximum redundancy though harder and more rigorous to set up. Less congestion, more efficient, more secure
* Full mesh would more likely be used in more important and larger organisations whereas partial mesh will be used for less large organisations.

Circuit switching:

* Method of data transmission
* Creates a direct physical link between devices
* Origins: originated with the first telephone networks in late 1800s
* E.g public telephone system, caller dials number, various switches in tp exchanges set up a connection
* If two computers use circuit switching principle, bandwidth is wasted during the periods when no data being sent. The two devices must also transmit and receive data at same rate
* Disadvantage – since switches are used to connect and disconnect circuit, electrical interference produced and although not serious for speech, may corrupt data.

Packet switching:

* Another method of data transmission
* Data is broken down into small packets, packets transmitted by itself and can take different routes to reach destination, which allows for less traffic across certain parts of networks as packets are evenly spread across network on their route to their destination.
* Large files broken down into smaller packets, of fixed size eg 1800 bytes for ethernet
* Last packet may be smaller if data is not evenly divisible.
* Packet consist of header, payload
* Header contains info like source, address, sequence number, checksum, protocol info
* Payload contains actual data
* Senders device breaks data into packets, each packet assigned sequence number, packets sent across network, receiver device reassembles the packets using sequence numbers
* Protocols used TCP and IP,
* Routers are used to connect at least two networks, commonly two LAN or wan, they determine best paths for packets to travel from source to destination
* Gateway act as gatekeepers between different networks often translating protocols to ensure compatibility. They can connect networks that use different protocols

Protocol:

* Set of rules which define methods of data communication and must be standard across all devices for communication.
  + HTTP/S – a client – server protocol which is the underlying protocol of www and defines how hypertext is transferred over internet, S is a extension of http which utilises encryption and authentication to provide secure communication.
  + FTP – file transfer protocol, a method of transferring data over a network, using a client server model
  + Mail server – program that sends messages from one mail client to another, stores incoming mail until it can be retrieved, takes advantages of protocols which tells the server how to process requests
  + POP – post office protocol, set of rules which retrieves emails from a mail server, temporarily stores incoming mail, once retrieved, transfers mail to your location.
  + Internet message access protocol IMAP – designed to keep emails on server
  + SIMple mail transfer protocol – SMTP used in transport of outgoing emails between servers or from clients to server

TCP/IP:

* TCP – transmission control protocol
* IP – internet protocol
* Encapsulation – adding layers to the packets, decapsulation is when the layers are stripped
* Application layer – at top of the TCP IP stack, decides which protocol will be used for data transmission.
* Transport layer – uses TCP to establish an end to end connection between source and the recipient computer. Breaks data into packets
* Network layer – forwards packets, adds MAC addresses so it is known which specific device data is sent to. So the MAC address first added, is the MAC address of the next router data goes to, then it is stripped and a different added, this new one indicates where the data hops to next, repeat until it reaches the final router which adds the MAC address of the specific device the data is going to.
* Link layer – handles actual data transmission