Section 02.1 - Networks Including the Internet

Layer 8: Networking

Syllabus Content Section 02: Communication

S02.1.1 Show understanding of the purpose and benefits of networking devices

---

`Sender`: The person giving / wanting to give data
`Receiver`: The person who will get the data
`Medium`: How yyu will sen it (WIFI,Cable) also called transmission medium
`Message`: What the data actually is
`Protocol`: The rules on how you will send

- Benefit
  - Easy to share information
  - More ways to learn
- Drawback
  - Share resources and devices
  - Requires setup and cost
  - Your data is vulnerable (virus, hackers)

S02.1.2 Show understanding of the characteristics of a LAN (local area network) and a WAN (wide area network)

`Wide area network (WAN)`: a network connecting computers on different sites, possibly thousands of
kilometres apart

- It will be used by an organisation or a company to connect sites or branches.
- It will not be owned by the organisation or company.
- It will be leased from a public switched telephone network company (PSTN).
- A dedicated communication link will be provided by the PSTN.
- The transmission medium will be fibre-optic cable.
- Transmission within the WAN will be from switch to switch.
- A switch will connect the WAN to each site.
- There will not be any end-systems connected directly to the WAN.

`Local area network (LAN)`: a network connecting computers in a single room, in a single building or
on a single site

- It will be used by an organisation or a company within a site or branch.
- It will be owned by the organisation or company.
- It will be one of many individual LANS at one site.
- The transmission medium will be twisted pair cable or WiFi.
- The LAN will contain a device that allows connection to other networks.
- There will be end-systems connected which will be user systems or servers.

S02.1.3 Explain the client-server and peer-to-peer models of networked computers

- Roles of the different computers within the network and subnetwork models
- Benefits and drawbacks of each model
- Justify the use of a model for a given situation

> `Client-server`: an architecture where a client runs an application provided by a server on a network
> Uses a server
> The server holds files centrally
> Can give access to those people who need it (authorisation and access control)
> Big businesses / lots of nodes

Has server
Has client (node that connects to server)
Best for networks with many nodes

- Benifits
  - Stable
  - If one machine breaks then the rest are okay
  - Access and authorisation control
- Drawbacks
  - More expensive than P2P
  - If server breaks then all machines cannot work
  - More difficult to install and setup

> `Peer to Peer(p2p)`:
> Nothing central
> Computers all connect to each other directly
> All computers share the same resources
> Better for home networks / small number of nodes

Best for networks with few nodes
Each node acts as a client AND a server

- Benifits
  - Simple setup
  - Cheap
- Drawbacks
  - No access control
  - If one computer breaks then the connecting ones cannot work

> `Point to Point`: is the same as Peer to Peer.
> But Point to Point is only with two nodes.

Best if you only need to communicate between you and one other node
Each node acts as a client AND a server

- Benifits
  - Simple setup
  - Cheap
- Drawbacks
  - No access control
  - If one computer breaks then the connecting ones cannot work

S02.1.4 Show understanding of thin-client and thick-client and the differences between them

---

`Thin-client`: a client that only provides input and receives output from the application

- chooses an application to run on the server
- sends input data to the server when requested by the application
- receives output from the application.

`Thick-client`: a client that carries out at least some of the processing itself

- chooses an application provided by the server
- possibly carries out some processing before running the application on the server and
  also aft er receiving output from the application
- alternatively, possibly downloads the application from the server and runs the application itself.

> Differences

Thick client is just a client that can still do things without a server. Things like store files, run apps / programs. If you can do these without the server then you have a thick client

A thin client is a client that NEEDS the server for everything. All your files and programs are stored on the server.

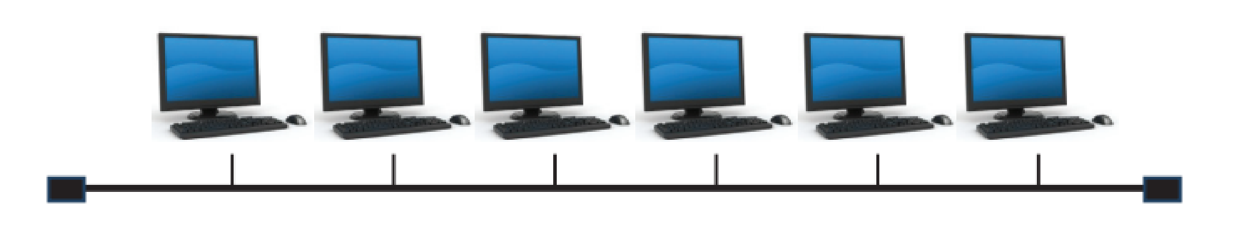
S02.1.5 Show understanding of the bus, star, mesh and hybrid topologies

- Understand how packets are transmitted between two hosts for a given topology
- Justify the use of a topology for a given situation

> `Bus topology`: contains one shared link to which all devices are attached

- Benifits
  - Simple
  - Can have more devices than point-to-point
  - If one device fails the rest of network is okay
  - Cheap because you need less cable
  - Easy to add a device
- Drawbacks
  - If backbone fails the network fails
  - If a terminator fails then network fails - High chance of collision because all data is sent on backbone

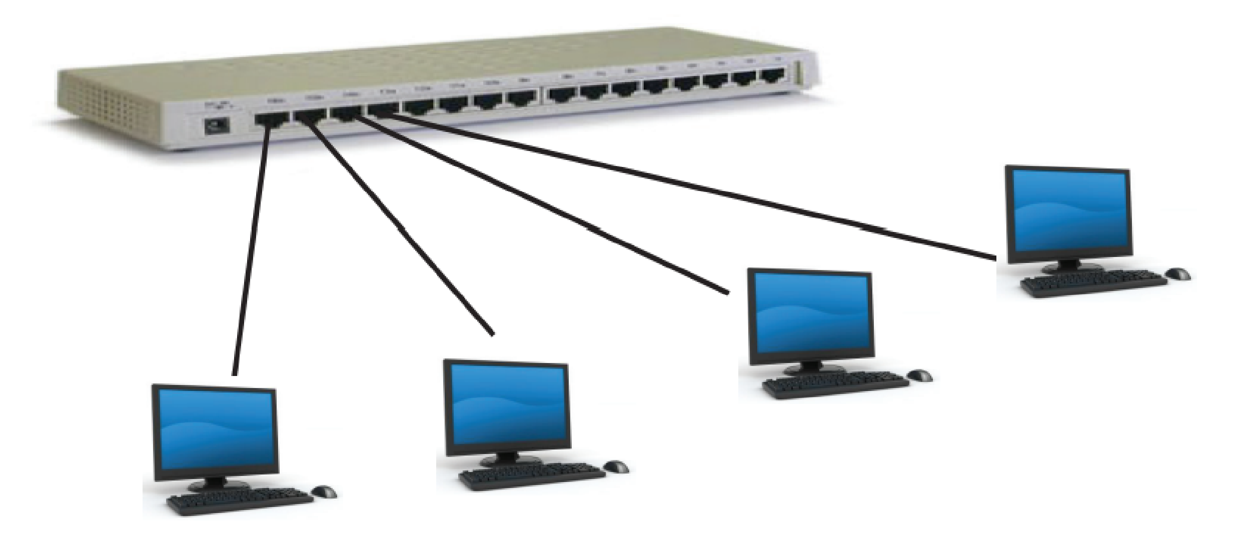
± All computers have equal priority to send data



> `Star topology`: each end-system is linked to a central device

- Benifits
  - Easy to add devices (as long as central device has space)
  - Can control the flow and access of data
  - If a device or cable fails, network is ok
- Drawbacks
  - If central device fails, network fails
  - Extra cost for central device

± Devices can send data at same time, the central device will handle the 'traffic'

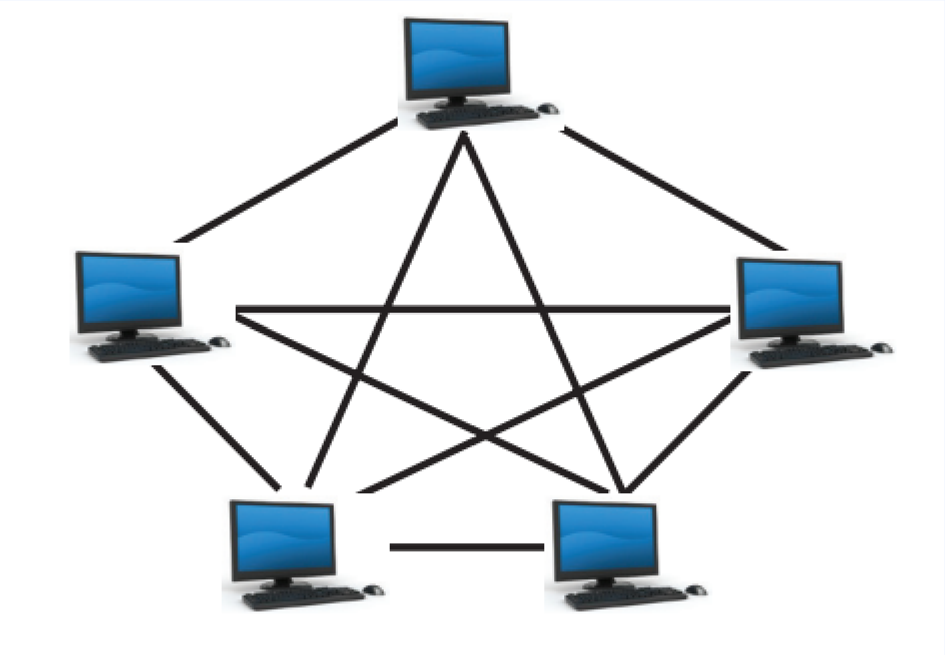


`Mesh topology`: contains direct links between devices

Popular with file sharing (torrents)
Usually one of the nodes is a server

- Benifits
  - If one device fails the network is okay
  - If one cable fails then network is okay

- Drawbacks
    - Little security control
    - Viruses are widespread



`Hybrid network`: a collection of connected LANs where some of them have diff erent topologies or supporting technologies

S02.1.6 Show understanding of cloud computing

- Including the use of public and private clouds.
- Benefits and drawbacks of cloud computing

`Private cloud`: owned by and only accessed by an organisation

- The organisation takes full responsibility for creating and managing the cloud installed
  on-site and connected to a private network
- The organisation outsources to a third-party the creation and management of an on-site
  installation connected to a private network

- The organisation outsources the creation and management of an Internet accessible
  system by a third-party.

`Public cloud`: owned by a cloud service provider for general access

- infrastructure provision
- platform provision
- soft ware provision

S02.1.7 Show understanding of the differences between and implications of the use of wireless and wired networks

- Describe the characteristics of copper cable, fibreoptic cable, radio waves (including WiFi), microwaves, satellites

---

> Wired networks

	Twisted pair	Coaxial	Fibre-optic
Cost	Lowest	Higher	Highest
Bandwidth or data rate	Lowest	Higher	Much higher
Attenuation at high frequency	Affected	Most affected	Least affected
Interference	Worst affected	Less affected	Least affected
Need for repeaters	More often	More often	Less often

> Wireless networks

`Wireless`: a transmission using radio, microwave or infrared

> relative advantages of transmission through a cable or wireless transmission.

- The use of certain wireless transmission frequencies is regulated by government agencies and so permission has to be obtained before wireless transmission is used.
- Outside these frequencies, no permission is needed to use the air for transmission but cables can only be laid in the ground with the permission of landowners.
- For global communications, the two competing technologies are: transmission through fibre-optic cables laid underground (or on the sea bed) and satellite transmission (discussed later in this section).
- Interference is much more significant for wireless transmission and its extent is dependent on which frequencies are being used for different applications.
- Repeaters are needed less often for wireless transmission.
- Mobile (cell) phones now dominate Internet use and for these, only wireless transmission is possible.
- For home or small office use, wired or wireless transmission is equally efficient; often, not having to install cables favours wireless connections for a small network.

S02.1.8 Describe the hardware that is used to support a LAN

- Including switch, server, Network Interface Card (NIC), Wireless Network Interface Card (WNIC), Wireless Access Points (WAP), cables, bridge, repeater

---

`switch`: a connecting device that can send a unicast message
`server`: a system providing a service to end-systems
`Network Interface Card (NIC)`: a component used to identify the end-system

`Wireless Network Interface Card (WNIC)`: provides the NIC function in a WiFi LAN
`Wireless Access Points (WAP)`: the connecting device in a WiFi LAN
`cables`: Copper Cable, Twisted Pair / Ethernet, Fibre Optic
`bridge`: a device that connects two segments of a LAN
`repeater`: a device that connects two cables and provides a full-strength signal to the second cable

S02.1.9 Describe the role and function of a router in a network

---

`Router`: a device that acts as a node on the Internet. Connects your LAN to another LAN

S02.1.10 Show understanding of Ethernet and how collisions are detected and avoided

- Including Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

S02.1.11 Show understanding of bit streaming

- Methods of bit streaming, i.e. real-time and on-demand
- Importance of bit rates/broadband speed on bit streaming

> `On-demand`: when the bit stream content is transmitted at a time chosen by the user

Someone uploads a video to a server.
You go on a website and can play it.
The website server starts to send you the data in a stream

Like Youku, BiliBili, YouTube, Netflix
Play, Pause, Forward and Rewind as you wish

> `Real-time`: when the bit stream content is transmitted as it is produced

Real time is the same as live streaming
A signal is being sent live and you receive it live.
Like a webcam show / online lesson
Or FaceTime / Skype call
It cannot be repeated again

> `Bit rate`: the number of bits transmitted per second

ABR = Adaptive Bitrate Streaming is when a video is encoded in different quality

When you want a video and watch it on your phone it runs at a certain bitrate, watch it on a TV and it'll run on a different bitrate

Bitrate depends on:
Screen size
Network speed
Size of buffer

S02.1.12 Show understanding of the differences between the World Wide Web (WWW) and the internet

---

> Internet

A group of computers
A connected group of computers, a network
A global connection of networks
A network of networks

> World wide web (www)

The Internet is computers connected together
The world wide web (WWW) USES the internet to send information
The information it sends is website information
HTTP – HyperText Transfer Protocol
You can use the internet for other things….like remote printing, email, torrents….

S02.1.13 Describe the hardware that is used to support the internet

- Including modems, PSTN (Public Switched Telephone Network), dedicated lines, cell phone network

---

> PSTN (Public Switched Telephone Network)

- Refers to all telephone networks
- Channel used between 2 endpoints for the call duration via circuit switching
- Lines active even during power outage
- Bi-directional communication

> Dedicated lines

- Telecommunication path between endpoints
- Not shared with multiple users; it's bought/leased
- Able to host websites as well as carry phone calls
- Allows continuous, uninterrupted access on Web

> Cell phone network

- Wireless network spread over land areas divided into (hexagonal) 'cells'
- Each cell is served by at least one base station (transceiver), which uses a different frequency range, as compared to adjacent cells, to transmit data

- Larger capacity possible since same frequencies can be used, in non-adjacent cells
- Radio waves are usually used for transmission
- Can be broadcast in all directions over a wide area
- Portable transceivers (e.g. mobile phones) are able to communicate and access internet via base stations

S02.1.14 Explain the use of IP addresses in the transmission of data over the internet

Including:

- format of an IP address including IPv4 and IPv6
- use of subnetting in a network
- how an IP address is associated with a device on a network
- difference between a public IP address and a private IP address and the implications for security
- difference between a static IP address and a dynamic IP address

---

There are two types of IP addresses:

$$IPv4 - IP\ Version4 - 2^{32}\ bits - 4,294,967,296\ combinations$$
$$IPv6 - IP\ Version6 - 2^{128}\ bits - 3.403x10^{38}\ combinations$$

IPv4	IPv6
32 bit address, split into 4 blocks by “.”	128 bit address divided into eight 16-bit blocks by “:”.
Each block could have a value between 0 and 255 (00 to FF in hex).	Each block can have 4 hex values ranging from 0000 to FFFF
E.g.255.0.1.255	IPv6 can be shortened by removing >=2 blocks containing solely zeroesE.g.2001:0db8:85a3::8a2e:0070:7334

IPv4 functionality

- each IP address has 2 parts:
  - Network Identifier (netID)
  - Identifies the network to which the host (device) is connected to
  - Host Identifier (hostID): Identifies the host within the network
- 'Classfull' addressing used for IPv4 where different bit lengths for identification and impose restrictions on available address

Subnetting

- Practice of dividing a network into two or more networks
- IP addresses are broken down to 3 parts by not changing the netID but partitioning the host ID into a subnet ID and host ID
- These subnet ID bits are used to identify each subnet within the network.
- Subnet masks are numbers that hides (masks) the netID of a system's IP address and leaves only the host part as the machine identifier, allowing data to be routed within the subnet to the appropriate host.

Public and Private IP address

- Public IP is provided by the ISP while Private IP issued by the LAN's router
- Public IP is unique and can be across the internet whereas Private IP is only unique within LAN and hence can only be accessed within LAN
- NAT (Network address translation) required for private IP addresses to access internet directly.
- Private IP more secure than public IP, since they are not directly accessible on the Internet and are hidden by NAT
- Range of IP addresses used for private IP addressing can never be assigned to public IP addresses

Static vs. Dynamic IP addresses

Static	Dynamic

Static	Dynamic
IP address never changes.	IP address will change at regular time periods.
Static IP addresses are useful when websites need to remember a device for a long time. Eg) VPNs whitelisting	Dynamic IP address is relatively more secure, hence used where data privacy is important
Faster upload/download speeds	Maintaining cost of dynamic IP address is lesser

S02.1.15 Explain how a Uniform Resource Locator (URL) is used to locate a resource on the World Wide Web (WWW) and the role of the Domain Name Service (DNS)

- `URL` (Uniform Resource Locator)
  - Unique reference address for the exact location of an internet resource on the WWW
- `Protocol`: enables browser to know what protocol is used to access info in domain
- `Hostname`: Domain name
- `Location of server`: path
- `Domain Name Service` (DNS)
  - naming system used for computers or resources having internet connection
  - Consists of a hierarchy of DNS servers which have a URLs database of and their corresponding IP addresses