2.1 Networking EMK Notes

Objective:

- Show understanding of **purpose** and **benefits** of networking devices.
- Show understanding of **characteristics** of a **LAN** and a **WAN.**
- Explain **client-server** and **peer-to-peer** models of networked computers.
- Roles of different computers within network and subnetwork models. Benefits and drawbacks of each model. Justify use of a model for a given situation.
- Show understanding of **thin-client** and **thick-client** and differences between them.
- Show understanding of **bus**, **star**, **mesh** and **hybrid** topologies. Understand how packets are transmitted between two hosts in given topology. Justify use of topology for given situation.
- Show understanding of differences between and implications of use of **wireless** and wired networks. Describe characteristics of copper cable, fiber optic cable, radio waves (including WiFi), microwaves, satellites.
- Describe hardware that is used to support a LAN. Including switch, server, Network Interface Card, Wireless Network Interface Card, Wireless Access Points , cables, bridge, repeater.
- Describe role and function of a router in a network.

What is Network?

"Network is a **linked set** of two or more computer systems, which may be capable of sharing **computer resources** such as printers, CD-ROM and databases."

Networks may be wired or wireless.

Category of Networks

- **Private networks** are owned by a **single company** or **organisation** (they are LANs or intranets with restricted user access, for example, passwords and user ids are required to join network).
- **Public networks** are owned by a **communications** carrier company (such as a telecoms company); many organisations will use network and there are usually no specific password requirements to enter network – but sub-networks may be under security management.

Benefit of Networking (Rather than using stand-alone computers)

- Devices, such as printers, can be shared thus **reducing costs**.
- **Licenses** to run software on networks are far **cheaper** than buying licences for an

equivalent number of **stand-alone computers**.

- Users can **share files** and **data.**
- Access to **reliable data** that comes from a central source, such as a **file server**.
- Data and files can be **backed up** centrally at end of each day.
- Users can **communicate** using email and instant messaging.
- Network manager can **oversee network** and apply **access rights** to certain files, or **restrict access** to external networks, such as internet.

Drawback of using Networking

- Cabling and servers can be an **expensive** initial outlay.
- Managing a large network can be a **complex** and **difficult task**.
- A **breakdown of devices**, such as the file servers, can affect whole network.
- **Malware** and **hacking** can affect entire networks.

Wide Area Network (WAN)

Wide area networks (WANs) are used when computers or networks are situated a **long distance** from each other (e.g they may be in different cities or on different continents). If a number of **LANs** are joined together using a **router** or **modem**, they can form a **WAN**.
Example of WAN: Network of automated teller machines (ATMs) used by banks.

Benefits of having Computers connected by a WAN:

- 'job' could be run on a remote computer that had the required application software
- **Data archive** that was stored on a remote computer could be accessed.
- A message could be **transmitted electronically** to a user on a remote computer.

Characteristic of WAN:

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

WANS have **slowest data communication** rates and **largest distances** could be thousands of kilometres apart.

2.1 Networking EMK Notes

Local Area Network (LAN)

LANs are usually contained within one building, or within a small geographical area. A typical LAN consists of a number of computers and devices (such as printers) connected to **hubs** or **switches**.

One of the hubs or switches is usually connected to a **router** and/or **modem** to allow LAN to connect to the internet or become part of a wide area network (WAN).

Hub is hardware device used to connect together a number of devices to form a LAN; directs incoming data packets to **all** devices on the network (LAN).

Switch is hardware device used to connect together a number of devices to form a LAN; directs incoming data packets to **a specific** destination address only.

Router is hardware device which enables data packets to be routed between different networks (for example, can join LANs to form a WAN).

Modem is modulator demodulator; device which converts digital data to analogue data (to be sent down a telephone wire); conversely it converts analogue data to digital data (which a computer can process).

Benefits of connecting PCs in a LAN:

M/J 2023-P12

- **Expense** of installing application software on each individual PC could be saved by installing software on an **application server** attached to LAN instead.
- Allow **sharing of file**. **File server** could be attached to LAN that allowed users to store larger files and also allowed files to be shared between users.
- Allow **sharing of resources**. Instead of supplying individual **printers** to be connected to a user's PC, one or more printers could be attached to **print server** that was connected to LAN.
- Allow Central Management e.g backup / security.
- Managers in organizations could use **electronic mail** to communicate with staff rather than sending round memos on paper.
- **'Paper-less office'** became a possibility, where files were to be stored in digital form on a **file server** rather than as paper copies in a filing cabinet.

Give three Main Characteristics LAN.

M/J 2023-P12

- It will be used by an organization or a company **within a site** or branch.
- LAN Cover small geographical area.

- It will be **owned by organization** or company.
- Transmission medium will be twisted pair cable or Wi-Fi.
- LAN will contain a **device** that allows connection to other networks.
- There will be end-systems connected which will be user systems or servers.

Wireless LANs (**WLAN**s) are similar to LANs but there are **no wires** or cables. Provide wireless network communications over fairly **short distances** (up to 100 metres) using **radio** or **infrared** signals.

Size of a Different Type of Network:
WAN: 100 km to over 1000 km (Wide Area Network)
MAN: 1 km to 100 km (metropolitan area network)
LAN: 10 m to 1000 m (Local Area Network)
PAN: 1 m to 10 m (Personal Area Network)

Word Internet is a shortened form of term '**internetwork'**, which describes number of networks all connected together.

Client-Server Model

Client-server model uses separate dedicated **servers** and specific **client** workstations; client computers will be connected to server computer(s).

- Users are able to access most of files, which are stored on dedicated servers.
- Server dictates which users are able to access which files. (Note: sharing of data is most important part of the client-server model.)
- Client-server model allows **installation** of software onto a **client**'s computer.
- The model uses **central security databases** which control access to the shared resources. (**Note**: passwords and user IDs are required to log into the network.)
- Once a user is logged into the system, they will have access to only those resources and files assigned to them by the network administrator, so offers **greater security** than peer-to-peer networks.
- Client-server networks can be as large as you want them to be and they are much **easier** to **scale up** than peer-to-peer networks.
- A central server looks after the storing, delivery and sending of emails.
- Client-server model offers most **stable system**, for example, if someone deletes a shared resource from server, **back-up** would restore deleted resource.
- Client-server network can become **bottlenecked** if there are several client requests at time.

- In **Client-Server Model**, a **file server** is used and is **responsible** for
  - Central storage and management of data files, thus enabling other network users to access files.
  - Allowing users to share information without the need for offline devices (such as a memory stick)
  - Allowing any computer to be configured as **host machine** and act as file server (note that server could be a storage device (such as SSD or HDD) that could also serve as a **Remote Storage** device for other computers, thus allowing them to access this device as if it were a local storage device attached to their computer).

Examples of use of Client-Server network model

A company/user would choose a **client-server** network model for following reasons.

- The company/user has a **large user-base** (This network model may still be used by a small group of people who are doing independent projects but need to have sharing of data and access to data outside the group).
- Access to **network resources** needs to be properly controlled.
- There is a need for good **network security**.
- Company requires its data to be free from **accidental loss** (Data needs to be backed up at a central location).

Peer-to-Peer model

Peer-to-peer is type of network in which **each node** can **share** its files with all other nodes. Each node has its **own data** and there is no **central** server. Because there is **no central storage**, there is no requirement to **authenticate** users.

Node is a device connected to network (it can be computer, storage or peripheral device).

On a Peer-To-Peer network, each node joins network to allow;

- **Provision of Services** to all other network users; services available are listed on nominated **'look up'** computer – when a **node** requests a service, **'look up'** computer is contacted to find out which of other network nodes can provide required service.
- Other users on network to simply **access data** from another node.
- **Communication** with other peers connected to network.
- Peers to be both **suppliers** and **consumers** (unlike client-server model where consumers and resources are kept entirely separate from each other).
- **Peers** to **participate** as **equals** on network (this is different to client-server model where a webserver and client have different responsibilities).

Peer to Peer model is used in scenarios where **few number of nodes** are required (small business) where it is **relatively easy** for users to be in contact with each other. More number of nodes leads to **performance** and **management** issues.

Peer-to-peer network offers little **data security** since there is no **central** security system. This means it is impossible to know who is authorized to **share certain data**.

In **Peer to Peer network** users can create their own network node **share point** which is only **real security** aspect since this gives them some kind of control. However, there are no **Real authentication** procedures.

Examples of peer-to-peer network model:

A user would choose peer-to-peer network model for one following reasons:

- Network of users is **fairly small**.
- There is no need for **robust security**.
- They require **workstation-based applications** rather than being **server-based**.

An **example** would be a small business where there is frequent user interaction and there is no need to have features of a **client-server** network.

Peer-to-peer model advantages	Client-Server Model advantages
It avoids possibility of congestion on network when many clients are simultaneously attempting to download files	It allows an organisation to control downloading and use of files.
Parts of a file can be downloaded separately.	Files can be better protected from malware attacks because files are stored on one server which will be regularly scanned using appropriate anti-virus software.
Parts are available from more than one host.	

Types of Clients

Client-server model offers **thin clients** and **Thick clients**. These can often refer to both **Hardware** and **Software.**

Thin Client

Thin Client can either be a device or software which needs to be connected to a **powerful** computer or **server** to allow processing to take place. Thin client will not work unless it is connected at all times to computer or server.

Example of Thin Clients:

- **Software** example would be a **Web browser** which has very limited functions unless it is connected to a server.
- Other examples is **mobile phone apps** which need constant access to a **server** to work.

- **Hardware** example is a **POS** terminal at a supermarket that needs constant access to a **server** to find prices, charge customers and to do any significant processing.

Pros and Cons of using Thin Client	
Pros	**Cons**
Less expensive to expand (low powered and cheap devices can be used)	High reliance on the server; if the server goes down or there is a break in communication link then the devices cannot work.
All devices are linked to a server (data updates and new software installation done centrally)	Despite cheaper hardware, the start-up costs are generally higher than for thick clients.
Server can offer protection against hacking and malware.	

Thick Client Server performs minimal processing for client. clients do most of their own processing independently. most of the resources are installed locally. Thick client can either be device or software that can work **offline** or **online**. It is still able to do some processing whether it is connected to a server or not.

Example of Thick Client:

- **Hardware example** is a normal PC/laptop since it would have its own storage, RAM and operating system which means it is capable of operating effectively online or offline.
- **Software Example** is computer game which can run independently on a user's computer, but can also connect to an online server to allow gamers to play and communicate with each other.

Pros and Cons of using Thick Client	
Pros	**Cons**
More robust. device can carry out processing even when not connected to server.	Less secure (relies on clients to keep their own data secure)
Clients have more control (they can store their own programs and data/files)	Each client needs to update data and software individually
	Data **integrity** issues, As many clients access same data which can lead to inconsistencies.

Differences between thick and thin client software	
Thin client software	**Thick client software**
Always relies on a connection to a remote server or computer for it to work.	Can run some of the features of the software even when not connected to a server.

Requires very few local resources (SSD, RAM memory or CPU processing time).	Relies heavily on local resources.
Relies on a good, stable and fast network connection for it to work.	More tolerant of a slow network connection
Data is stored on remote server or computer.	Can store data on local resources such as HDD or SSD.

ESQ: Network runs as thick-client model. Describe what is meant by a thick-client model.

Networked Computers

Networked computers form an **infrastructure** which enables **internal** and **external** communications to take place. The infrastructure includes the following:

Hardware	Software	Services
• LAN cards • routers • switches • wireless routers • cabling	•Operation and management of the network • operation of firewalls • security applications /utilities	• DSL • Satellite communication channels • Wireless protocols • IP addressing.

Five requirements for a data communications system are a sender, a receiver, a transmission medium, a message and a protocol.

Types of transmission mode on bases of Direction of data

Simplex Data Transmission:

Simplex is **one direction** data transmission from transmitter (sender) to receiver.

Example:

(a) Data from **keyboard to your CPU**.

(b) Data being sent from a computer to a printer.

(c) Another example are Television, or Radio.

Half-Duplex Data Transmission:

It is transmission of data in **both** directions but not at the same time. An **example** of a half-duplex system is **walkie-talkie**.

Full-Duplex Data Transmission:

It is transmission of data in **both** directions simultaneously. It is also known as **duplex** data transmission.

Example:

1) Broadband connection on a phone line.

2) Telephone is a full-duplex device because both parties can talk at once.

Type of Message

When a message is sent it can be as a broadcast, a multicast or a unicast.

Unicast Message:

Communication technique in which data transmission is done between two devices is known as **Unicast**. It is also known as **one to one** or **point to point** communication.

Example: Communication between server and client.

Multicast Message:

Communication technique in which **data transmission** is done between a particular **group** of devices is known as Multicast. This is similar to **group message** that we send through SMS or sending e-mail to a particular mailing group.

Broadcast:

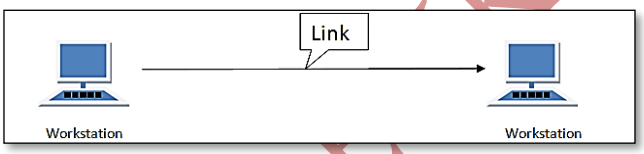
Communication where a piece of information is sent from **one point** to all other points. In this case there is just one sender, but information is sent to all connected receivers.

Network Topologies

There are **many** ways to connect computers to make complex networks.

❖ **Point-to-Point Connection :**

Simplest possible network is where two end-systems are connected by a network link. Transmission might be simplex or duplex and a message can only be **unicast**.

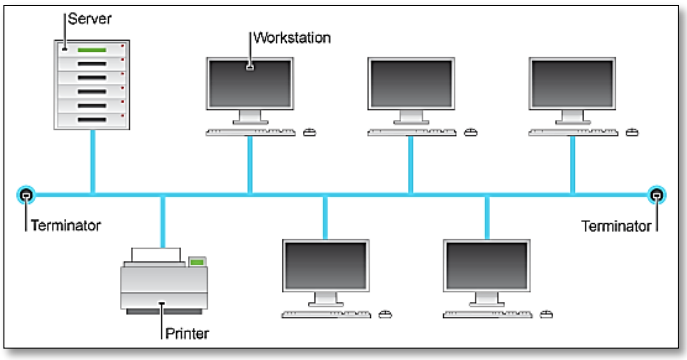


❖ **Bus Topology:**

A bus topology has only **one link** but it is shared by number of end-systems and is described as a **multi-point connection**. There is no **direct connection** between any pair of end systems. A message must be **broadcast** even though it might only be intended for one end-system.

Bus topology is resilient because a fault in an end-system or in the link to it does not affect the use of the network by the other end-systems.

Advantages	Disadvantages
• Even if one node fails, the remainder of the network continues to function. • It is easy to increase the size of the network by adding additional nodes.	•If main cable fails, whole network goes down. • Performance of network declines under heavy loading. • Network is **not secure** since each packet passes through every node.



How packets are transmitted in Bus Topology?

In bus network topology, each node looks at each packet and determines whether or not the address of the recipient in the package matches the node address. If so, the node accepts the packet; if not, the packet is ignored.

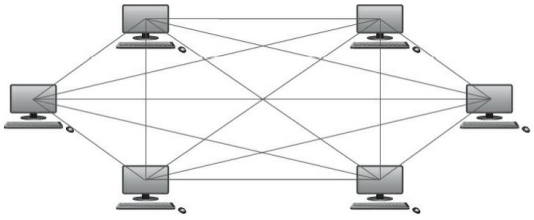
Bus Topology is most suitable for situations with a small number of devices with light traffic occurring. For example, a small company or an office environment.

❖ **Mesh Topology:**

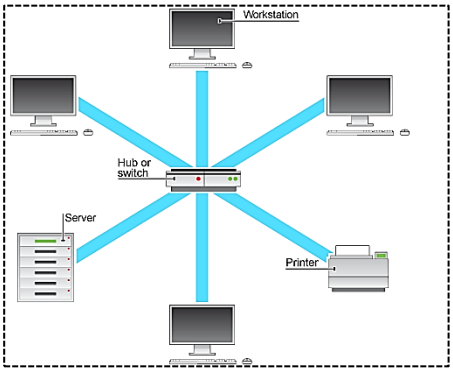
In this configuration, each end-system has a point-to-point connection to each of the other end systems. Transmission is duplex; messages might be unicast, multicast or broadcast.

M**esh topology** can be used when individual LAN switches are connected in a network. The topology is essential for the connection of **routers** within the infrastructure of the Internet.

Disadvantages of A Mesh Network	Advantages of A Mesh Network
Large amount of cabling is needed, which is expensive and time consuming.	It is easy to identify where faults on the network have occurred.
Set-up and maintenance is difficult and complex.	Any broken links in the network do not affect the other nodes.
	The network is relatively easy to expand.



❖ **Star Networks:**



In star topology, each end system has **point-to-point** connection to **central device**. Transmission is **duplex** and messages from central device might be **unicast, multicast or broadcast**. Failure of an end-system, or its link, leaves other

end-systems unaffected. However, central device must not fail. **Central Device** is specialized device (server etc) with purpose of connecting other devices in network. Currently, star topology is usual way to configure a network.

Advantages of A Star Network	Disadvantages of star network
Data collisions are greatly reduced due to the topology.	If central hub/switch fails, then whole network goes down.
More **secure** network since security methods can be applied to **central node** and packets only travel to nodes with correct address.	Initial installation costs are high.

ESQ: How packets are handled in Star topology?

How packets are handled depends on whether the central node is a switch or a hub. If it is a **hub**, all the packets will be sent to every device/node on the star network – if the address in the packet matches that of the node, it will be accepted; otherwise, it is ignored. If the central node is a **switch**, packets will only be sent to nodes where the address matches the recipient address in the packet.

Star Networks are useful for evolving networks where devices are frequently added or removed. They are well suited to applications where there is **heavy** data traffic.

Hybrid Networks:

Hybrid network is mixture of **two** or more **different topologies** (bus and star, bus and mesh, and so on). Main advantages and disadvantages depend on which types of network are used to make up hybrid network, but main disadvantage is that they can be very **complex** to install, configure and maintain.

Transmission Media

Twisted pair Cable:

Twisted pair cables are most common cable type used in LANs. It has **lowest data transfer** rate and suffers most from **external interference** (such as electromagnetic radiation). However, it is **cheapest** option. Twisted pair use **copper** for transmission medium.

Types of twisted pair cable:

- **Unshielded** is used by residential users.
- **Shielded** is used commercially (Cable contains thin metal foil jacket which cancel out some of external interference).

Coaxial Cables:

Coaxial cables are most commonly used cables in **MANs** and by cable television companies. **Cost** of coaxial cables is **higher** than twisted pair cables but they offer better **data transfer rate** and are affected **less** by external interference. Coaxial cables also

have about 80 time transmission capacity of twisted pair. It is not usually used for **long-distance** telephone cabling.

Fibre Optic Cables:

Fibre optic cables are commonly used to send data over **long** distances, because they offer **best data transfer rate**, smallest **signal attenuation** and have a very **high resistance** to external interference.

Main drawback is **high cost**. Fibre optics use **pulses of light** rather than pulses of electricity to transmit data. They have about 26000 times transmission capacity of twisted pair cables.

Types of Fiber Optic Cable:

- **Single-mode Fiber Optic Cable** uses a **single mode light** source and has a smaller central core, which results in less light reflection along cable. This allows data to **travel faster** and making them a good choice for **telecommunications.**
- **Multi core Fiber Optic Cable** allows for **multi-mode** light source; construction causes higher light reflections in core, so they work best over **shorter distances** (in a LAN).

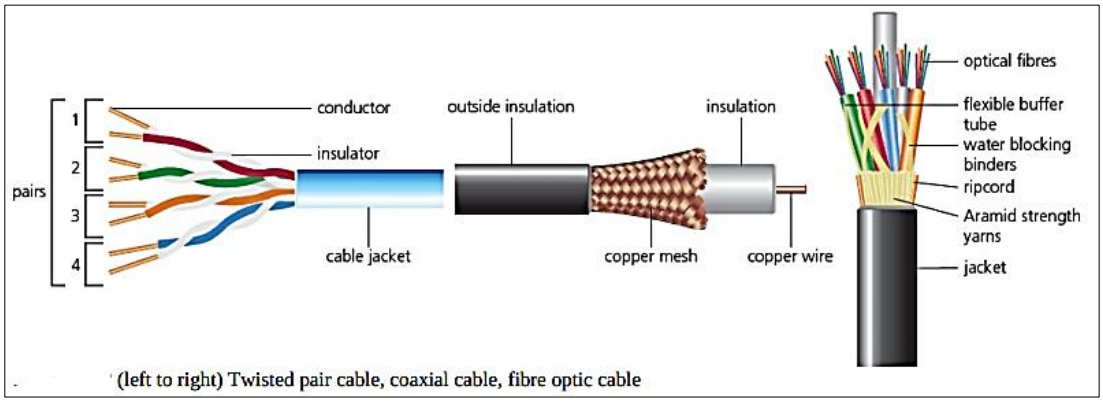
	Twisted pair	Coaxial	Fibre-optic
Cost	Lowest	Higher	Highest
Bandwidth or data rate	Lowest	Higher	Much higher
Attenuation at high frequency	Affected	Most affected	Least affected
Interference	Worst affected	Less affected	Least affected
Need for repeaters	More often	More often	Less often

Suitability for given Application:

- **Cost** of cable and connecting devices.
- Best **bandwidth** that can be achieved. Bandwidth governs possible data transmission rate.

Factors Causing Poor Performance of Cables:

- **Interference** affecting transmitted signals.
- Extent of **attenuation** (deterioration of signal) when high frequencies are transmitted. When a signal is transmitted at a high frequency, it can experience more attenuation compared to a low-frequency signal.



(left to right) Twisted pair cable, coaxial cable, fibre optic cable

Wireless Transmission

It is transmission using electromagnetic radiation (radio, microwave or infrared).

Frequency range	Radio 3 kHz–3 GHz	Microwave 3–300 GHz	Infrared 300 GHz–400 THz
Bandwidth or data rate	→	→	→
Attenuation (mainly due to rain)	→	→	→
Need for repeaters	→	→	→
Directional focusing capability	→	→	→
Penetration through a wall	←	←	←
Interference	There is no systematic trend		

- **Penetration** measures ability of electromagnetic radiation to pass through different media.

  Radio waves **>** microwaves **>** infrared (radio waves have best penetration)

- **Attenuation** is reduction in amplitude of a signal. Infrared has low attenuation because it can be affected by rain or internal walls. Thus infrared is best suitable for **indoor** use only. Fact that it can be stopped by walls is seen as an advantage since this stops signal causing **interference** elsewhere.
- **Bandwidth:** It is measure of the **amount of data** that can be transmitted per second.

  infrared **>** microwaves **>** radio waves (infrared has largest bandwidth)

Wired versus Wireless

- **Wired Networking**
  - More **reliable** and **stable** network.
  - **Data transfer** rates tend to be faster.
  - Tends to be **cheaper** overall, in spite of the need to buy and install cable.
  - Devices are **not mobile**; they must be close enough to allow for cable connections.
  - Lots of wires can lead to **tripping hazards**, overheating of connections.

- Permission from authorities and land owners is required before laying cables underground.

Wireless Networking:

- It is easier to **expand networks** and is not necessary to connect devices using cables.
- Devices have **increased mobility**, provided they are within range of the WAPs.
- Increased chance of **interference** from external sources.
- Data is **less secure** than with wired systems; it is easier to intercept radio waves and microwaves than cables.
- Data transmission rate is **slower** than wired networks.
- Signals can be stopped by **thick walls**.

Wi-Fi and Bluetooth

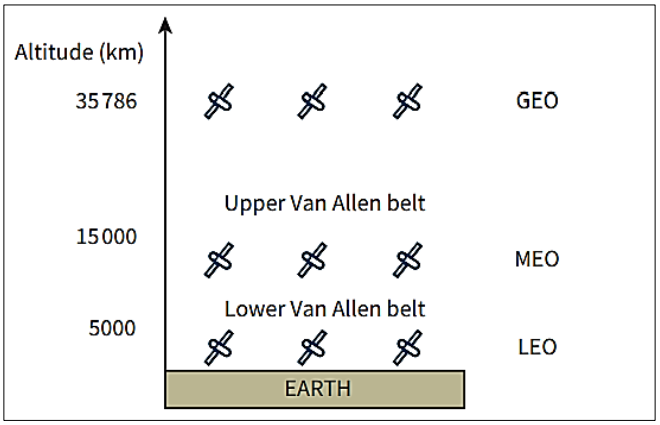
Wi-Fi and Bluetooth offer wireless communication between devices. They both use **electromagnetic radiation** as carrier of data transmission.

Bluetooth sends and receives **radio waves** in band of 79 different frequencies (channels). Devices using Bluetooth automatically detect and connect to each other, but they do not interfere with other devices since each **communicating pair** uses different channel. When a device wants to communicate, it picks one of 79 channels at random. If channel is already being used, it randomly picks another channel. This is known as **Spread Spectrum Frequency** hopping.

Wi-Fi uses **spread spectrum** technology. Wi-Fi is best suited to operating full-scale networks, since it offers much **faster data transfer rates**, better **range** and **better security** than Bluetooth. Wi-Fi-enabled device (computer or smart phone) can access, internet Wirelessly at any wireless access point (WAP) or 'hot spot' up to 100 metres away.

Satellites

Satellites are components of modern **communication systems**. Van Allen belts are areas containing high levels of electrically charged particles, which interfere with satellites.



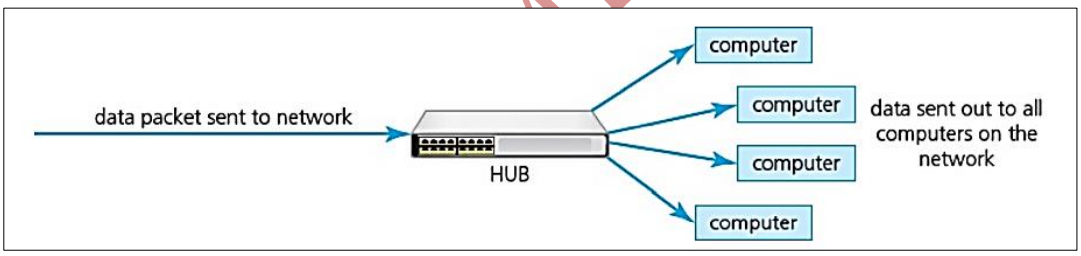
- **GEO Satellites: Highest altitude** satellites are in geostationary Earth orbit (GEO) over equator and these are used to provide **long-distance telephone** and computer **network** communication. 'Geostationary' means that satellite orbits at same speed as Earth spins,. Only **three** GEO satellites are needed for full global coverage.
- **MEO Satellite:** Closer to Earth are a group of medium Earth-orbit (MEO) satellites some of which provide the global positioning system (GPS). **Ten** MEO satellites are needed for global coverage.
- **LEO Satellites:** Low-Earth-orbit (LEO) satellites work in 'constellations' to supplement the mobile phone networks. **Fifty** LEO satellites are needed for full global coverage but currently there are several hundred LEO satellites in orbit.

Satellite can act as a component in a network and can directly connect with ground-based components.

Disadvantage of satellites is that the greater transmission distance causes transmission delays, which can cause technical problems for the network.

Hardware Requirements of LAN Networks

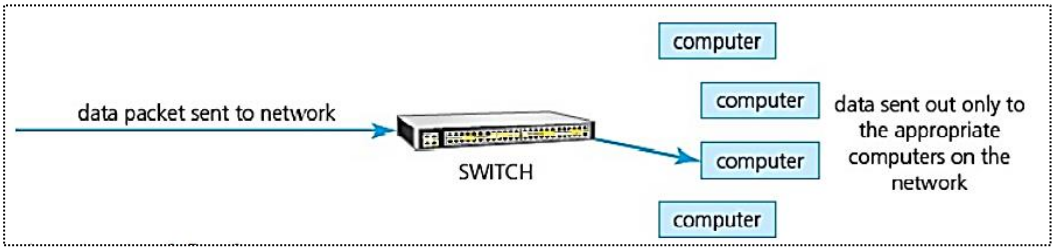
- **Hub:** Hubs are hardware devices that can have a number of devices or computers connected to them.



Its **main task** is to take any data packet received at one of its ports and then send the data to every computer in the network. Using hubs is not a very **secure** method of data distribution and is also **wasteful** of bandwidth. Hubs can be wired or wireless devices.

- **Switch:**

Switch connect a number of computers together to form a LAN. Unlike a hub, the switch checks the data packet received and works out its destination address and sends the data to the appropriate computer only. This makes using a switch a more **secure** and e**fficient** way of distributing data.



Each device on a network has a **MAC** address which identifies it **uniquely**. Data packets sent to switches will have a MAC address identifying the source of the data and additional addresses identifying each device which should receive the data. Switches can be wired or wireless devices.

Repeater:

When signals are sent over long distances, they suffer attenuation or signal loss. Repeaters are devices which are added to transmission systems to boost the signal so it can travel greater distances. They amplify signals on both analogue (copper cable) and digital (fibre optic cable) communication links.

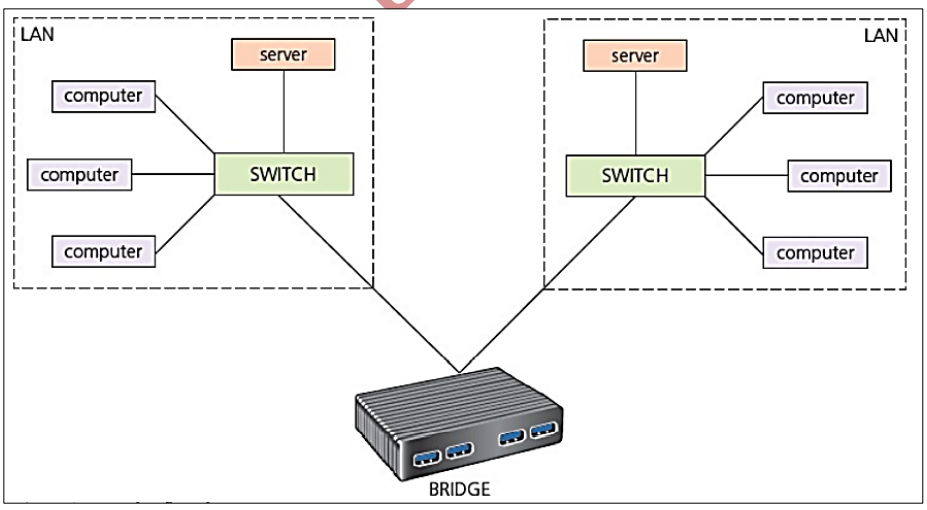
Repeaters can also be used on wireless systems. These are used to boost signals to prevent any 'dead spots' in the Wi-Fi zone.

Sometimes, **hubs** contain repeaters and are known as **repeating hubs**. All signals fed to the hub are boosted before being sent to all devices in the network, thus increasing the operational range.

Bridge

Bridges are devices that connect one LAN to another LAN that uses same **protocol.** They are often used to connect together different parts of a LAN so that they can function as a single LAN.

Bridges can be wired or wireless devices. Bridge stores network addresses for end-systems in two segments it connects.



Router

Routers enable data packets to be **routed** between **different networks** for example, to join a LAN to a WAN. Router takes data transmitted in one format from a network and converts data to a protocol and format understood by another network, thereby allowing them to communicate via router.

Role of routers as follows;

- Restrict broadcasts to a LAN.
- Act as a default gateway
- Can perform **protocol translation**; for example, allowing a wired network to communicate with a wireless (Wi-Fi) network – router can take an Ethernet data packet, remove Ethernet part and put IP address into a frame recognised by wireless protocol.
- Can move data between networks.
- Can calculate **best route** to a network destination address.

Gateway:

It is a network point that acts as an **entrance to another network**. It can be used to connect two or more dissimilar LANs (LANs using different protocols). Gateway converts data packets from one protocol to another. Gateways can also act as routers, firewalls or servers – in other words, any device that allows traffic to flow in and out of the networks. Gateways can be wired or wireless devices.

All networks have boundaries so that all communication within network is conducted using devices such as switches or routers. If a network node needs to communicate outside its network, it needs to use a gateway.

Modems:

Modern computers work with digital data, whereas many of the public communication channels still only allow analogue data transmission. To allow the transmission of digital data over analogue communication channels we need to use a modem (modulator demodulator). Modem converts **digital data** to **analogue data**. It also does the reverse and converts data received over the analogue network into digital data which can be understood by the computer.

Wireless modems transmit data in a modulated form to allow several simultaneous wireless communications to take place without interfering with each other.

Network Interface Card (NIC)

Network interface card (NIC) is needed to allow a device to connect to a network (such as the internet). It is usually part of the device hardware and frequently contains the MAC address generated at the manufacturing stage.

Wireless network interface card/controller (WNIC)

WNICs are same as NICs, in that they are used to connect devices to internet or other networks. They use an **antenna** to communicate with networks via microwaves and normally simply plug into a USB port or can be internal integrated circuit plug in.

Differences between routers and gateways

Routers	Gateways
• forward packets of data from one network to another; routers read each incoming packet of data and decide where to forward the packet	• convert one protocol (or data format) to another protocol (format) used in a different network
• can route traffic from one network to another network	• convert data packets from one protocol to another; they act as an entry and exit point to networks
• can be used to join LANs together to form a WAN (sometimes called brouters) and also to connect a number of LANs to the internet	• translate from one protocol to another
• offer additional features such as dynamic routing (ability to forward data by different routes)	• do not support dynamic routing

Public switched telephone network (PSTN)

During early years of networking, telephone network carried **analogue voice data**. However, digital data could be transmitted provided that a modem was used to convert digital data to analogue signals. Another modem was used to reverse process at receiving end. Such 'dial-up' connections provided **modest-speed**, **shared access** when required.

More recently, PSTNs have upgraded their main communication lines to **fibre-optic cable** employing **digital** technology. This has allowed to offer improved leased line services to ISPs. There are two **types of service**. The first is a **broadband network** connection for traditional network access. Second is **WiFi hotspot** technology, where an access point has a connection to a wired network providing Internet access.

Example Telephone calls can be made by using:

- **Conventional telephones (PSTN) over a wired network**
- **Computer, equipped with speakers and microphone, connected to the Internet**

Put tick in correct column to match description to appropriate communication method.

Ans:

Description	Conventional telephone using PSTN	Internet-based system
connection only in use whilst sound is being transmitted		✓
dedicated channel used between two points for the duration of the call	✓	
connection maintained throughout the telephone call	✓	
encoding schemes and compression technology used		✓
lines remain active even during a power outage	✓	

****

Exam Style Questions

ESQ#1 One of company's offices one server and four computers connected in a star topology. Draw a diagram to show layout of office's star topology. **M/J/23 P12**

Ans: