Chapter 2 Communication

2.1 Networks Including the Internet

2.1 Networks including the internet	
Candidates should be able to:	Notes and guidance
Show understanding of the purpose and benefits of networking devices	
Show understanding of the characteristics of a LAN (local area network) and a WAN (wide area network)	
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
Show understanding of thin-client and thick-client and the differences between them	
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
Show understanding of cloud computing	Including the use of public and private clouds. Benefits and drawbacks of cloud computing
Show understanding of the differences between and implications of the use of wireless and wired networks	Describe the characteristics of copper cable, fibre-optic cable, radio waves (including WiFi), microwaves, satellites
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
Describe the role and function of a router in a network	
Show understanding of Ethernet and how collisions are detected and avoided	Including Carrier Sense Multiple Access / Collision Detection (CSMA / CD)
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
Show understanding of the differences between the World Wide Web (WWW) and the internet	
Describe the hardware that is used to support the internet	Including modems, PSTN (Public Switched Telephone Network), dedicated lines, cell phone network

A networking device is a hardware device that is used to connect multiple computers or other devices together to form a network. The purpose of networking devices is to enable communication and data sharing between devices within a network.

The benefits of networking devices include:

Improved Communication: Networking devices enable communication between devices within a network, allowing for real-time collaboration and sharing of information.

Resource Sharing: Networking devices allow for the sharing of resources such as printers, scanners, and internet connections, reducing costs and improving efficiency.

Increased Security: Networking devices can help to improve network security by providing features such as firewalls, access controls, and encryption.

Scalability: Networking devices can easily be added or removed from a network, allowing for easy scalability as a network grows or changes.

Centralized Management: Networking devices can be managed centrally, making it easier to configure and monitor a network.

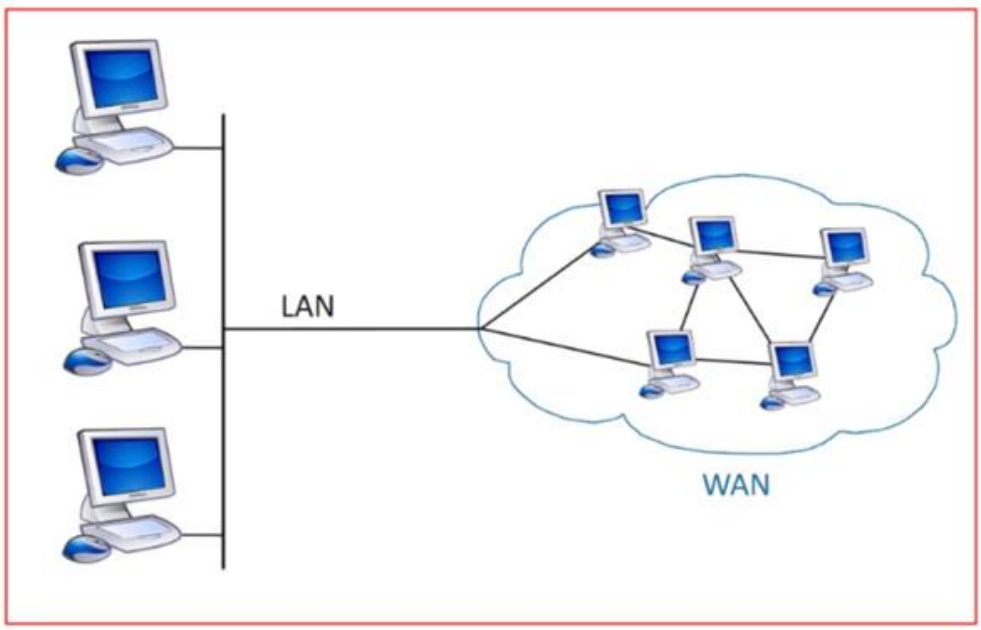
LAN / WAN

LAN

- Devices connected over a small geographical area
- company-owned infrastructure // Uses dedicated infrastructure // No leasing external infrastructure / transmission media // does not use internet to transmit within the building

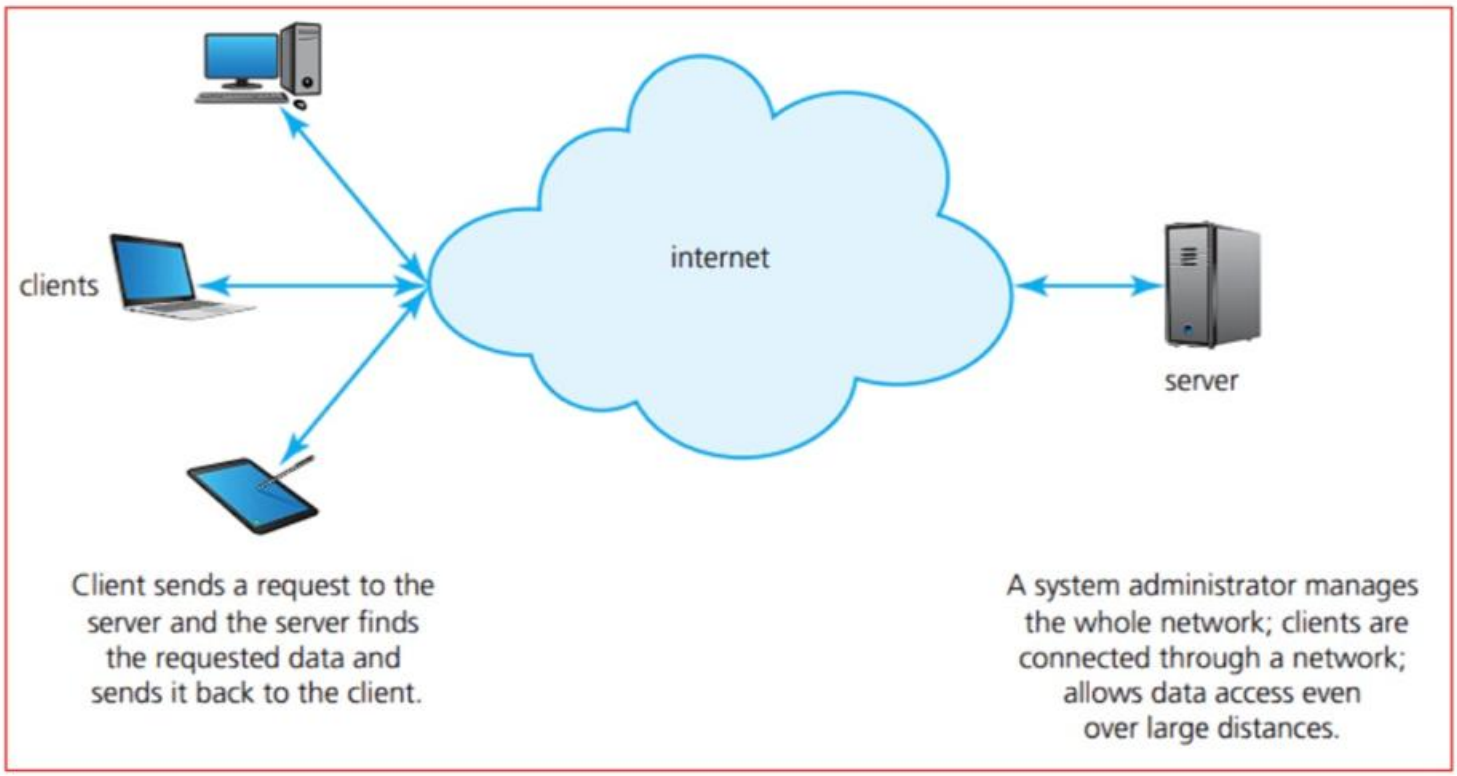
WAN

- A network connecting computers on different sites, possibly thousands of kilometers apart



Network Models

Client-Server



- There's at least one computer which acts as a server
- Other computers are referred to as clients
- Client requests resources/services from the server
- Server provides services/resources/applications/files

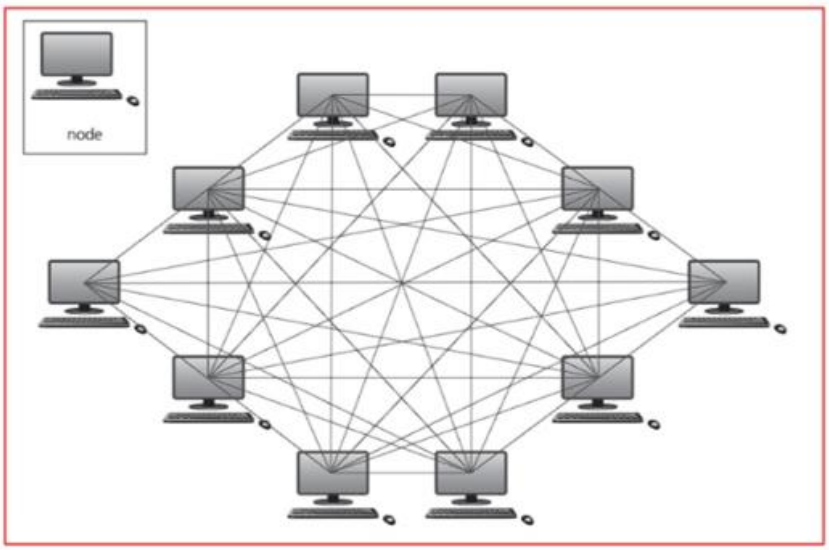
Webpage	Bank
• User's browser is the client • The file is made available from the server • Client requests for the file • The desired file is returned to the client computer	• The information of the user is stored on the server • The user's computer/browser acts as the client • It sends a request to the server via browser • The server responds with the information requested by the user • E.g. recent transactions, current account balance, any due payments

Benefits	Drawbacks
✓ Centralized storage of data, data can be accessed from any workstation/computer ✓ Centralized backup ✓ Creation of security ✓ Internet monitoring ✓ Clients can be less powerful, low specification devices, cheaper to set up ✓ Saving resources on server reduces burden on client ✓ Access rights can be assigned to users	✓ Single point of failure: The client-server model is vulnerable to a single point of failure. If the server goes down or becomes unavailable, clients may not be able to access the resources or services they need. ✓ Scalability: The scalability of the client-server model can be an issue, as the server may become overwhelmed if too many clients try to access it simultaneously. This can result in slow response times or even server crashes. ✓ Security: The client-server model can be vulnerable to security breaches if the server is not properly secured. For example, if a hacker gains access to the server, they can potentially access all the data stored on it and compromise the system. ✓ Cost: Implementing a client-server architecture can be expensive, as it requires the use of dedicated servers and specialized software. ✓ Complexity: The client-server model can be complex to implement and maintain, especially in large networks. It requires expertise in server administration, networking, and security to ensure that everything is running smoothly.

Examples of use of client-server network model

- Using a printing server
- Using a file server
- School or office with centralized storage of data
- Access to network resources needs to be properly controlled
- There is a need for good network security.
- The company requires its data to be free from accidental loss (in other words, data needs to be backed up at a central location).

Peer to Peer



- Each node is connected to all other nodes in the network
- All nodes can communicate with each other
- Each node is of equal status in the network
- Each node can share files to all nodes in the network
- Each node can access files from all nodes in the network
- All nodes are responsible for their own security

Benefits	Drawbacks
✓ It avoids the possibility of congestion when more clients are simultaneously requesting to download a file. ✓ It allows the user to download different parts of files separately. ✓ The parts are available from more than one host.	✓ Reduced Security, Any virus on any computer can be transmitted to all other nodes ✓ No central backup of data, if the node storing some specific data gets damaged for some reason data is lost. ✓ In order to share files, all the computers must be on, otherwise files cannot be shared, this means that files aren't accessible always

Examples of peer-to-peer network model

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

Thin clients & Thick clients

Thin Client

A thin client is heavily dependent on having access to a server to allow constant access to files and to allow applications to run uninterrupted. A 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 (the computer or server could be on the internet or could be part of a LAN/MAN/WAN network). The thin client will not work unless it is connected at all times to the computer or server. A software example would be a web browser which has very limited functions unless it is connected to a server. Other examples include mobile phone apps which need constant access to a server to work. A 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.

Thick Client

A thick client can either be a 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. A thick client can either be connected to a LAN/MAN/WAN, virtual network, the internet or a cloud computing server. A hardware example is a normal PC/laptop/tablet since it would have its own storage (HDD or SSD), RAM and operating system which means it is capable of operating effectively online or offline. An example of software is a 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	Cons
Thick Clients	✓ more robust (device can carry out processing even when not connected to server) ✓ clients have more control (they can store their own programs and data/files	✓ less secure (relies on clients to keep their own data secure) ✓ each client needs to update data and software individually ✓ data integrity issues, since many clients access the same data which can lead to inconsistencies
Thin Clients	✓ less expensive to expand (low-powered and cheap devices can be used) ✓ all devices are linked to a server (data updates and new software installation done centrally) ✓ server can offer protection against hacking and malware	✓ high reliance on the server; if the server goes down or there is a break in the communication link then the devices cannot work ✓ despite cheaper hardware, the start-up costs are generally higher than for thick clients

Thick Client	Thin Client
• can run some of the features of the software even when not connected to a server download a file. • relies heavily on local resources • more tolerant of a slow network connection • can store data on local resources such as HDD or SSD	• always relies on a connection to a remote server or computer for it to work • requires very few local resources (such as SSD, RAM memory or computer processing time) • relies on a good, stable and fast network connection for it to work • data is stored on a remote server or computer

TOPOLOGY

A network topology is the arrangement with which computer system are connected to each other.

BUS TOPOLOGY:

Uses a single central cable to which all computers and devices are connected.

Benefits	Drawbacks
✓ Easier to set up ✓ Less cable required ✓ Less expensive	✓ If the main cable breaks, network problem degrades badly. ✓ Difficult to detect and troubleshoot fault at an individual station. ✓ Efficiency reduces as the number of devices connected to it increases. ✓ Collisions, not suitable for networks with heavy traffic. ✓ Security is lower because several computers receive the sent signal from the source.

How are packets transmitted between two computers in Bus Topology?

- Packets have the address of recipients.
- The sender transmits data through the bus.
- The bus carries data along the central cable.
- As the data arrives at each computer, the system compares the address to see if it matches.

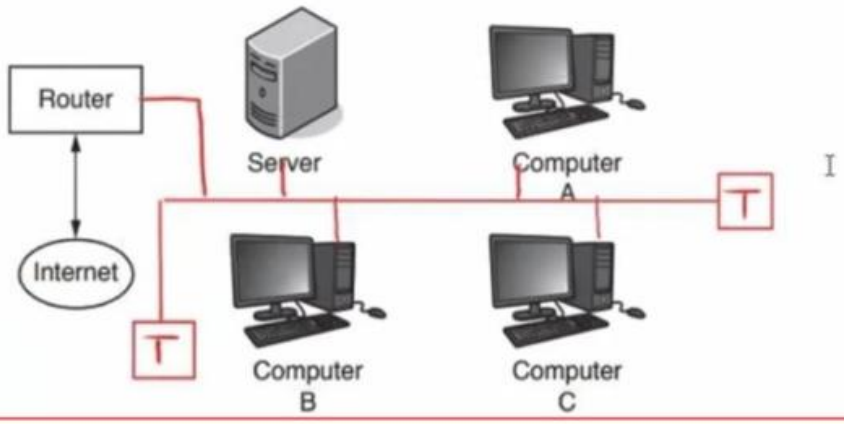
Where will we use bus topology?

- Used when small and temporary network is needed.
- Networks which does not rely on high data transfer speed.
- Used in office or schools.

Past Paper Question

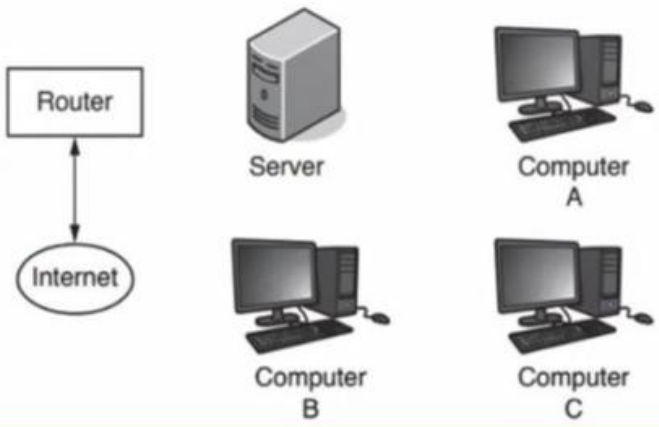
A Local Area Network (LAN) consists of three computers, one server and a router connected to the Internet. The LAN uses a bus topology.

(a) Complete the following diagram to show how the computers, the server and the router could be connected.



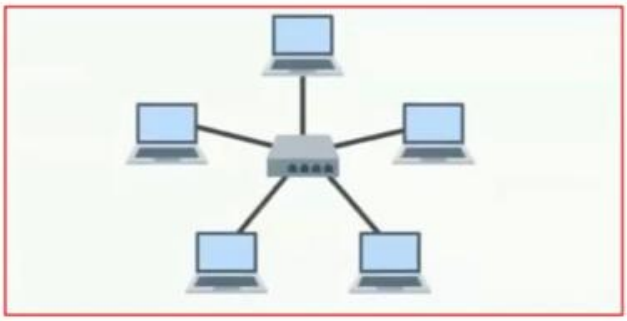
A Local Area Network (LAN) consists of three computers, one server and a router connected to the Internet. The LAN uses a bus topology.

(a) Complete the following diagram to show how the computers, the server and the router could be connected.



STAR TOPOLOGY:

Every computer is linked with central device.



Benefits	Drawbacks
✓ Signals only go to destinations so secure ✓ Easy to connect/remove node ✓ Centralized management helps in monitoring the network. ✓ Failure of one node or link doesn't affect the rest of the network. ✓ Fewer collisions	✓ If the central device fails then whole network goes down. ✓ Performance is dependent on capacity of central device.

How are packets transmitted between two computers in Star Topology?

- Packets have the address of recipients.
- Sender sends data to central devices.
- Server reads address and find where recipient is.
- Server directly sends data to recipient.
- Server transmits packets only to recipient.

Where will we use star topology?

- Large organizations
- Educational establishments
- Where high performance is must
- Found in homes as well where router acts as a server.

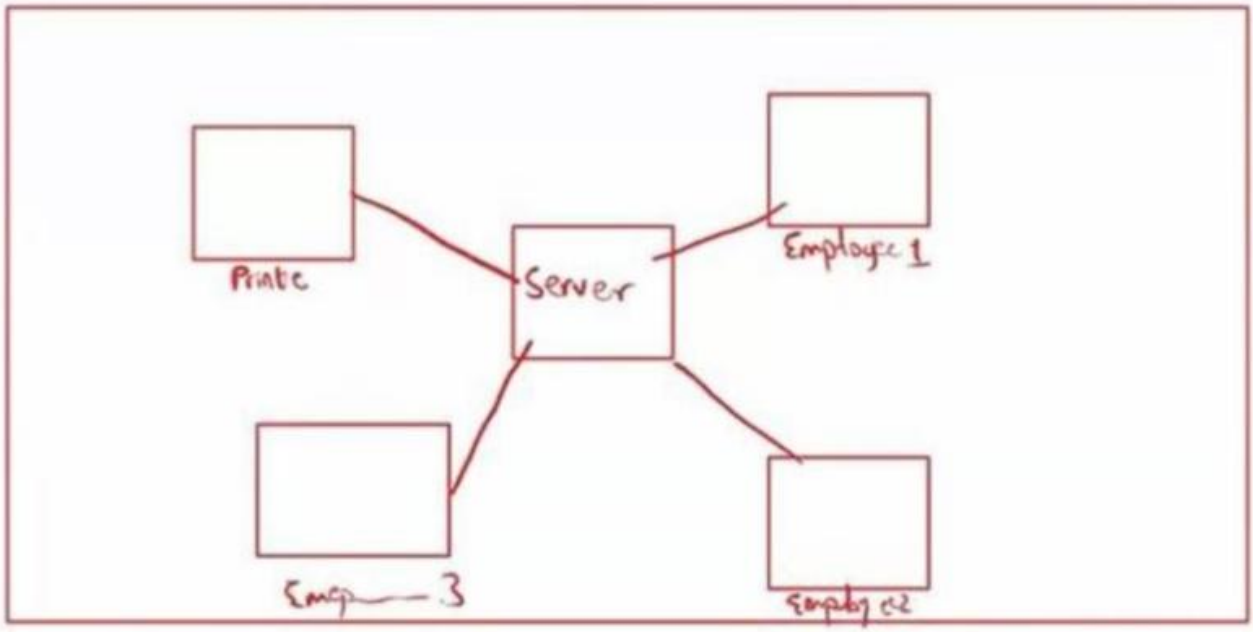
Features of Star Topology

- Must have a central device
- Each node is connected to the central device.
- Each node has a dedicated connection.
- Each connection must be bi-directional.

Past Paper Question

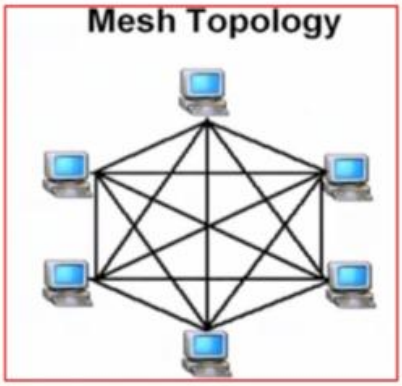
2 Cables connect the computers in a university admissions department in a star topology. The server room contains the server and printer for the employees to use. The department has three employees. Each employee has a computer connected to the star network.

(a) (i) Draw a diagram to show this topology.



MESH TOPOLOGY:

All the devices are interconnected to each other.



Benefits	Drawbacks
✓ Any broken links in the networks do not affect the other nodes. ✓ Good privacy and security, since packets travel along dedicated routes	✓ A large amount of cabling is needed, which is expensive and time-consuming. ✓ Setup and maintenance is difficult and complex.

How are packets transmitted between computers in Mesh Topology?

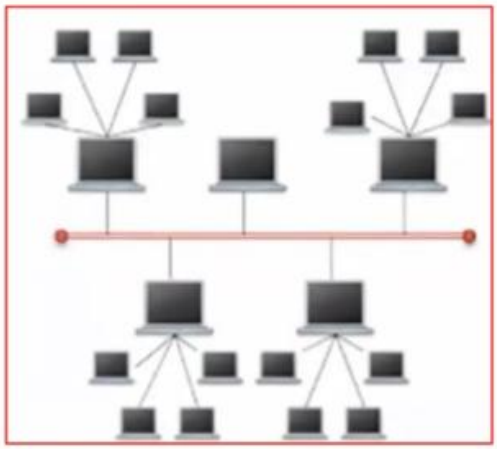
- Packets have addresses of recipients.
- Sender transmits packets directly to node.
- As each node is connected to at least one another node.

Where will we use mesh topology?

- Where establishment of communication is very important.
- Military organizations
- Emergency services

HYBRID TOPOLOGY:

All the devices are interconnected to each other.



Benefits	Drawbacks
✓ Highly reliable as in case of failure there are many sub networks. ✓ Easy to trouble shoot and fix errors.	✓ Cost, expensive to set up ✓ Difficult to manage ✓ Complex network

Where will we use hybrid topology?

Large organizations with different topologies in each building.

Cloud Computing

A physical server is located in an offsite location, with files/applications stored on it. It basically acts as a remote server.

Public Cloud

The firm or the company using the remote server to store the files, doesn't own the remote server, Owned by third party, and is available to anyone with an internet connection, and credentials. Computing services offered over the public network.

Private Cloud

A firm/company has purchased and installed a remote server to store their files/applications/software, and own the server. Only available to selected users, only accessible for the organization., computing services offered over internet or a private internal network.

Benefits	Drawbacks
✓ No need to store files on hard drive ✓ Files can be accessed from anywhere in the world, at any time from any device provided that internet connection is available ✓ Can acts as backup storage ✓ Data can be shared easily ✓ It can almost go unlimited ✓ Free for little amount of storage	✓ Cannot access files if lost internet ✓ Data is not secure, data breaches, no control over security ✓ The cloud server is a physical server located somewhere, it fails due to some natural disaster all data will be deleted, no control over backups ✓ Expensive for long term ✓ Have to pay for more storage

Wired & Wireless Network

Numerous factors should be considered when deciding if a network should use wired or wireless connectivity, as listed below.

Wireless Network

Benefits	Drawbacks
✓ Devices are more mobile; The network can be accessed from anywhere within range of an access point ✓ Easier to connect more devices ✓ Easy to set up, No cabling required ✓ Many devices can be connected at the same time ✓ Less hard wiring/hardware is required, Reduced cost of setting up the network ✓ No need to physically connect each device, It is much more straightforward to connect other devices	✓ Interference of signals ✓ Easier to hack ✓ Signals degrades quickly ✓ Transmissions may be less secure because data packets can be intercepted // easier connection by unauthorized user ✓ Bandwidth may be limited // As more devices connect the bandwidth can be reduced so access may be slow ✓ It is subject to interference from other signals or obstacles which can hinder transmission or corrupt data ✓ Limited range // greater attenuation so there is a need for repeaters // users can easily move out of range ✓ Higher latency so transmission will be slower

Wired

Benefits	Drawbacks
✓ More secure less interference ✓ Data transfer is faster ✓ Cheaper overall	✓ Devices not mobile ✓ Tripping hazards

Wi-Fi & Bluetooth

Both Wi-Fi and Bluetooth offer wireless communication between devices. They both use electromagnetic radiation as the carrier of data transmission. Bluetooth sends and receives radio waves in a band of 79 different frequencies (known as channels). These are all centered on a 2.45GHz frequency. Devices using Bluetooth automatically detect and connect to each other, but they do not interfere with other devices since each communicating pair uses a different channel (from the 79 options) When a device wants to communicate, it picks one of the 79 channels at random. If the channel is already being used, it randomly picks another channel. This is known as **spread spectrum frequency hopping**. To further minimize the risks of interference with other devices, the communication pairs constantly change the frequencies (channels) they are using (several times a second). Bluetooth creates a secure wireless personal area network (WPAN)
based on key encryption.

Bluetooth is useful when

- ✓ transferring data between two or more devices which are less than 30 meters apart
- ✓ the speed of data transmission is not critical
- ✓ using low bandwidth applications (for example, sending music files from a mobile phone to a headset).

As mentioned earlier in the chapter, Wi-Fi also uses **spread spectrum technology**. However, 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. A Wi-Fi-enabled device (such as a computer or smart phone) can access, for example, the internet wirelessly at any wireless access point (WAP) or 'hot spot' up to 100 meters away.

Satellites

Penetration : measures the ability of electromagnetic radiation to pass through different media.
Attenuation : the reduction in amplitude of a signal

The use of microwaves and radio waves was previously mentioned as a method for allowing Wi-Fi connectivity in networks. These methods are perfectly satisfactory for short distances – the electromagnetic waves carry the signals – but the curvature of the Earth prevents such methods transmitting data globally. The communication between antennae and satellite is carried out by radio waves or microwave frequencies. Different frequency bands are used to prevent signal interference and to allow networks spread across the Earth to communicate through use of satellites

Cables

Twisted pair cables

- most common cable type used in LANs
- lowest data transfer rate
- suffers the most from external interference
- cheapest option
- Unshielded is used by residential users. Shielded is used commercially

Benefits of Copper Cable (twisted pair)

- ✓ Cheaper to install
- ✓ Easy to set up
- ✓ Been around for years

Coaxial cables

- most commonly used cables in MANs (metropolitan area network (network which is larger than a LAN but smaller than a WAN, which can cover several buildings in a single city, such as a university campus)
- cost of coaxial cables is higher than twisted pair
- better data transfer rate than twisted pair

Fiber optic cables

- most commonly used to send data over long distances
- smallest signal attenuation
- very high resistance to external interference.
- high cost
- Fiber optic cables can be single- or multi-mode.1
    - Single mode uses a single mode light source and has a smaller central core, which results in less light reflection along the cable. This allows the data to travel faster and further, making them a good choice for CATV (community antenna television (CATV), these cable systems use a "community antenna" to receive broadcast signals (often from communications satellites)) and telecommunications.

    - Multi core allows for a multi-mode light source; the construction causes higher light reflections in the core, so they work best over shorter distances (in a LAN, for example).

Benefits	Drawbacks
✓ Greater security ✓ Greater bandwidth ✓ Need less signal boosting ✓ Lightweight ✓ Consume less power ✓ High resistance to signal attenuation ✓ Fastest data transfer rate	✓ Expensive to set up ✓ Requires expertise

Differences between fiber optic and copper cable

- Fiber optic data is transmitted using light, copper cable through electrical signals
- Fiber optic has higher bandwidth than copper cable
- Fiber optic has higher transmission rates than copper cable
- Fiber optic has smaller risk of (noise) interference than copper cable
- Fiber optic can be used over longer distances than copper cable before repeaters are needed
- Fiber optic is much more difficult to hack into than copper cable
- Fiber optic is more prone to damage than copper cable

Devices used to support a LAN

Router

- Connects two or more networks
- Can connect a network to a WAN
- Receives packets and forwards towards destination
- Assigns private IP addresses
- Operates between similar networks using same protocol
- Can be used to segment a network
- To store / update / maintain a routing table
- To find the most efficient path to the destination
- To maintain a table of MAC and IP addresses

Gateway

- Connects two or more networks
- Can connect a network to a WAN
- Receives packets and forwards towards destination
- Assigns private IP addresses
- Connects two dissimilar networks using different protocols

Switch

- they connect a number of devices or computers together to form a LAN (for example, a star network).
- However, unlike a hub, the switch checks the data packet received
- works out its destination address (or addresses)
- sends the data to the appropriate computer(s) only.
- makes using a switch a more secure and efficient way of distributing data

Wireless Network Adapter

- Hardware component that allows a device to connect to a wireless network
- Provide interface to wireless network
- … as an antenna
- Receives analogue radio waves
- … convert them to digital / binary
- Checks incoming transmissions for correct MAC / IP address
- … ignore transmissions not intended for it
- Encrypts / encodes the data • Decrypts / decodes the data
- Takes digital/binary input and converts to analogue waves
- … sends the radio waves via the antenna

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 (fiber 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.
- These devices plug into electric wall sockets and send out booster signals.
- They are termed non-logical devices because they will boost all signals which have been detected; they are
- not selective.

Bridge

- devices that connect one LAN to another LAN that uses the same protocol
- used to connect different parts of a LAN so that they can function as a single LAN.

Network interface card (NIC)

- needed to allow a device to connect to a network (such as the internet).
- usually part of the device hardware and frequently contains the MAC address generated at the manufacturing stage

Wireless Access Point (WAP)

Hardware component that provides radio communication from the central device to nodes on the network (and vice versa)

Ethernet

Ethernet is a protocol used by many wired LANs. It was adopted as a standard by the Institute of Electrical and Electronic Engineers (IEEE) and Ethernet is also known as IEEE 802.3.

A network using Ethernet is made up of:

- a node (any device on the LAN)
- medium (path used by the LAN devices, such as an Ethernet cable)
- frame (data is transmitted in frames which are made up of source address)

Conflicts

if devices on the same network have been given the same IP address; without a unique IP address it is not possible to connect to a network. This is most likely to occur on a LAN where dynamic IP addresses may have been used. can be resolved by re-starting the router. Any dynamic IP addresses will be re-assigned, which could resolve the issue.

CSMA/CD collision management

- CSMA/CD is a protocol used to detect and prevent collisions in a bus topology
- Workstations listen to the communication channel
- If no data is being transmitted, he computer frames as packet and transmits it
- Collision is caused when two messages are sent from the same channel at the same time
- As collision occurs a jamming signal is sent
- Transmission is terminated
- If collisions occur each workstation waits a random time before retransmitting
- Each time a collision occurs, random time is increased.

Bit Streaming

- Data is compressed before streaming
- Sequence of bits are streamed over the internet
- They require fast data transfer speed and fast broadband connection
- the bits are stored in the buffer and then played back for the user as they're downloaded from the dedicated streaming server
- Bits arrive in the same sequence as they were streamed

How is it possible to watch a video on web without it continually pausing

- Fast data transfer speed and fast broadband connection required
- Data is streamed to a buffer ○ The sequence of bits streamed are stored in buffer, and then broadcasted to user. The rate of data transfer to from web to buffer should be greater than rate of data transfer while broadcasting the video to user for it to not stop continuously
- As buffer is emptied it's filled up again so that viewing is continuous
- Actual playback of the video is a few seconds behind

Benefits	Drawbacks
✓ Any video file or music file can be played on demand ✓ No need to store video/music files on hard drive ✓ Better security, harder to copy streamed files then downloaded files ✓ No need to wait for entire video/music file to be downloaded to play it • No specialist software required to playback video in browser	✓ Requires high bandwidth ✓ Video lags/stops and waits for the buffer to get loaded, with an unstable internet connection or insufficient buffer capacity ✓ Viruses may be downloaded from websites ✓ Cannot access videos/music without internet ✓ Copyright issue

On Demand Streaming

- Digital video file is stored on the file server
- It's encoded into bit streaming format and uploaded on dedicated streaming server

- A link is available for the user on the website, through which user can download the file • User clicks on the link to download encoded streaming video
- As the file is streamed to the user, it's broadcasted to user.
- Video can be forwarded, rewound and paused.

Real Time Streaming

- An event is being captured with a video camera and microphone
- The video camera and microphone are connected to a computer
- Video signals encoded to streaming media files
- Encoded feed is then uploaded on a dedicated streaming server
- Cannot be paused/forwarded.

Differences between on-demand and real time bit streaming

- On demand: can be fast forwarded or paused.
- real time: streaming is live and cannot be fast forwarded or paused.

- On Demand: Digital video stored on server which is encoded into bit streaming format and uploaded to dedicated video server
- Real Time: Video captured real time from a video camera connected to a computer

- On Demand: Streaming of video that has been recorded in the past, recorded lessons etc.
- Real Time: Live real time streaming of any event that's currently taking place, e.g. a football match

World Wide Web (WWW) and the internet

Internet

- Massive network of networks/interconnected network of computer devices
- Internet stands for Interconnected Networks
- Uses TCP/IP protocol

World Wide Web

- Collection of multimedia web pages and documents
- .. stored on websites
- http protocol used to transmit data
- web pages are written in html
- URL's specify location of the webpages
- web documents are accessed using browsers.

Difference between Internet and WWW

- Internet is the infrastructure , the global collection of networks
- World Wide Web is collection of multimedia web page and documents, content
- World Wide Web is accessed over the internet
- Web pages are written in html
- Internet uses IP/TCP protocol, WWW uses HTTP protocol to transfer web pages

Supplementary Question

Ali is sending an email to his boss, using a website?, Is he using WWW or Internet, or both?

Answer: Obviously both, Internet is being used to the send data on the infrastructure, whereas the WWW used to access the website stored on webserver

Hardware used to support the internet

Transmission of Data using PSTN

- uses a standard telephone connected to a telephone line
- The telephone line connection is always open whether or not anybody is talking –
- the link is not terminated until the receivers are replaced by both parties.
- Telephone lines remain active even during a power cut; they have their own power source
- The PSTN consists of many different types of communication lines
- Data is transmitted in both directions at the same time, simultaneously, i.e. full duplex data transmission
- The communication passes through different switching centers.

Benefits	Drawbacks
✓ Faster Connection ✓ More consistent transmission speed ✓ Improved Security	✓ Expensive to set-up and maintain ✓ Disruption to the dedicated line would leave no alternative ✓ Outdated technology

Phone calls using the internet

Phone calls using the internet use either an internet phone or microphone and speakers (video calls also require a webcam).The internet connection is only 'live' while data (sound/video image) is being transmitted.

Voice over Internet Protocol (VoIP) converts sound to digital packages (encoding) which can be sent over the internet. VoIP uses packet switching; the networks simply send and retrieve data as it is needed so there is no dedicated line, unlike PSTN. Data is routed through thousands of possible pathways, allowing the fastest route to be determined. The conversation (data) is split into data packages. Each packet contains at least the sender's address, receiver's address and order number of packet – the sending computer sends the data to its router which sends the packets to another router, and so on. At the receiving end, the packets are reassembled into the original state (see Chapter 14 for more details).VoIP also carries out file compression to reduce the amount of data being transmitted. Because the link only exists while data is being transmitted, a typical 10-minute phone call may only contain about 3 minutes where people are talking; thus only 3MB of data is transmitted making it much more efficient than PSTN.

Cellular networks and satellites

Other devices, such as mobile phones, use the cellular network. Here, the mobile phone providers act as the ISPs and the phones contain communication software which allows them to access the telephone network and also permits them to make an internet connection. Satellites are an important part of all network communications that cover vast distances. Due to the curvature of the Earth, the height of the satellite's orbit determines how much coverage it can give. Figure 2.22 shows how satellites are classified according to how high they orbit in relation to the Earth's surface.

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). This device 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. A modem will connect to the public infrastructure (cable, telephone, fiber-optics or satellite) and will supply the user with a standard Ethernet output which allows connection to a router, thus enabling an internet connection to occur While the router will allow the creation of a network in a home, for example, the modem allows for the connection to the external networks (for example, the internet). Routers and modems can be combined into one unit; these devices have the electronics and software to provide both router and modem functions. Another example of a modem is a soft modem (software modem), which uses minimal hardware and uses software that runs on the host computer. The computer's resources (mainly the processor and RAM) replace the hardware of a conventional modem.

2.1 Networks Including the Internet Continued

2.1 Networks including the internet continued	
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
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)	

IPV4

- most common type of addressing on the internet
- This is based on 32bits giving 232 (4294 967296) possible addresses.
- 32 bits are split into four groups of 8bits (thus giving a range of 0 to 255).
- For example, 254.0.128.77.

The system uses the group of bits to define network (netID) and network host (hostID). The netID allows for initial transmission to be routed according to the netID and then the hostID is looked at by the receiving network. Networks are split into five different classes

Network class	IPv4 range	Number of netID bits	Number of hostID bits	Types of network
A	0.0.0.0 to 127.255.255.255	8	24	very large
B	128.0.0.0 to 191.255.255.255	16	16	medium size
C	192.0.0.0 to 223.255.255.255	24	8	small networks
D	224.0.0.0 to 239.255.255.255	–	–	multi-cast
E	240.0.0.0 to 255.255.255.255	–	–	experimental

Consider the class C network IP address 190.15.25.240, which would be written in binary as:

10111110 00001111 00011001 11110000

Here the **network** id is **190.15.25** and the **host ID** is **240**.

Consider the class B network IP address 128.148.12.14, which would be written in binary as:

10000000 10010100 00001100 00001110

Here the **network** ID is **128.148** and the **host ID** is **12.14** (made up of sub-net ID 12 and host ID of 14).

Consider the class A network IP address 29.68.0.43, which would be written in binary as:

00011101 01000100 00000000 00101011

Here the **network** ID is **29** and the **host ID** is **68.0.43** (made up of sub-net ID 68.0 and host ID of 43).

IPv6

- IPv6 addressing has been developed to overcome some of the problems associated with IPv4.
- uses 128-bit addressing
- IPv6 address is broken into 16-bit chunks
- it adopts the hexadecimal notation.
- For example: A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA
- colon (:) rather than a decimal point (.) is used here.
- designed to allow the internet to grow in terms of number of hosts

IPv6 has benefits over IPv4

- has no need for NATs (network address translation)
- removes risk of private IP address collisions
- has built in authentication
- allows for more efficient routing.

Zero compression

IPv6 addresses can be quite long; but there is a way to shorten them using zero compression. For example, 900B:3E4A:AE41:0000:0000:AFF7:DD44:F1FF can be written as:

900B:3E4A:AE41::AFF7:DD44:F1FF

With the section 0000:0000 replaced by ::

The zero compression can only be applied ONCE to an IPv6 address, otherwise it would be impossible to tell how many zeros were replaced on each occasion where it was applied. For example, 8055:F2F2:0000:0000:FFF1:0000:0000:DD04 can be rewritten either as:

8055:F2F2::FFF1:0000:0000:DD04

or as:
8055:F2F2:0000:0000:FFF1::DD04

Uses of subnetting

- Improved security
- Reduces congestion
- Allows extension of the network
- Aids day to day management
- Improves performance

What happens when a web page is requested by a user?

- User keys in the uniform resource locator (URL) into the browser software
- The Domain Name service uses the domain name from the browser to look up the IP address of the webserver
- The web server sends the web page content to the browser
- Browser software renders the page and displays *(If JavaScript is included then the client computer or the browser processes the JavaScript code and then the requested web page is displayed to user)*

How is URL converted to its matching IP address?

- Uniform Resource Locator (URL) us parsed to obtain the domain name
- Domain name is sent to the nearest domain name server (dns)
- Dns holds a list of domain names and matching ip addresses
- Dns name resolved searched its database for the domain name
- If dns does not find the domain name, the request is forwarded to a higher level dnss
- If the domain name is found, the ip address is returned
- If the domain name is not found the request is passed to a higher-level server
- If the domain name is finally not found, an error message is generated

Supplementary Question

Why the above IPV6 would be an invalid IPV4 address?

Answer: It's using colon as separators instead of dot, there are too many groups, IPV4 has only 4 groups some groups are more than 8 bits, the address is more than 32 bits overall. Too many digits per group

Public and Private IP address

- Public is assigned by an ISP
- Public IP addresses can be accessed by anyone using the Internet
- Public is used to get internet service
- Public IP addresses must be unique throughout the Internet

- Private is assigned by a router
- Private IP addresses cannot be accessed by anyone using the Internet
- Private is used to communicate within a network
- Private can be duplicated in different networks // private addresses are unique only within the (local) network

Purpose of an IP address

- Gives each device on network an identifier, can be used to locate a device on a network Each address is unique within the network
- Allows a device/gateway/node to send data to correct destination e.g. another device, gateway

Statement	Public IP Address	Private IP Address
192.168.2.1 is an example of this type of address		✓
Assigned by the ISP	✓	
IP address cannot be duplicated in different networks	✓	
Network address translation is necessary to access the internet directly		✓
The address can be reached over the internet	✓	
The address is more secure		✓
The address can only be accessed through the same LAN		✓
The address can be duplicated in different networks		✓

Static and Dynamic IP address

Static	Dynamic
When a computer disconnects and joins the network back the IP address is unchanged, it's assigned by the ISP	Each time the computer rejoins the network, the address changes, address is assigned by the network OS