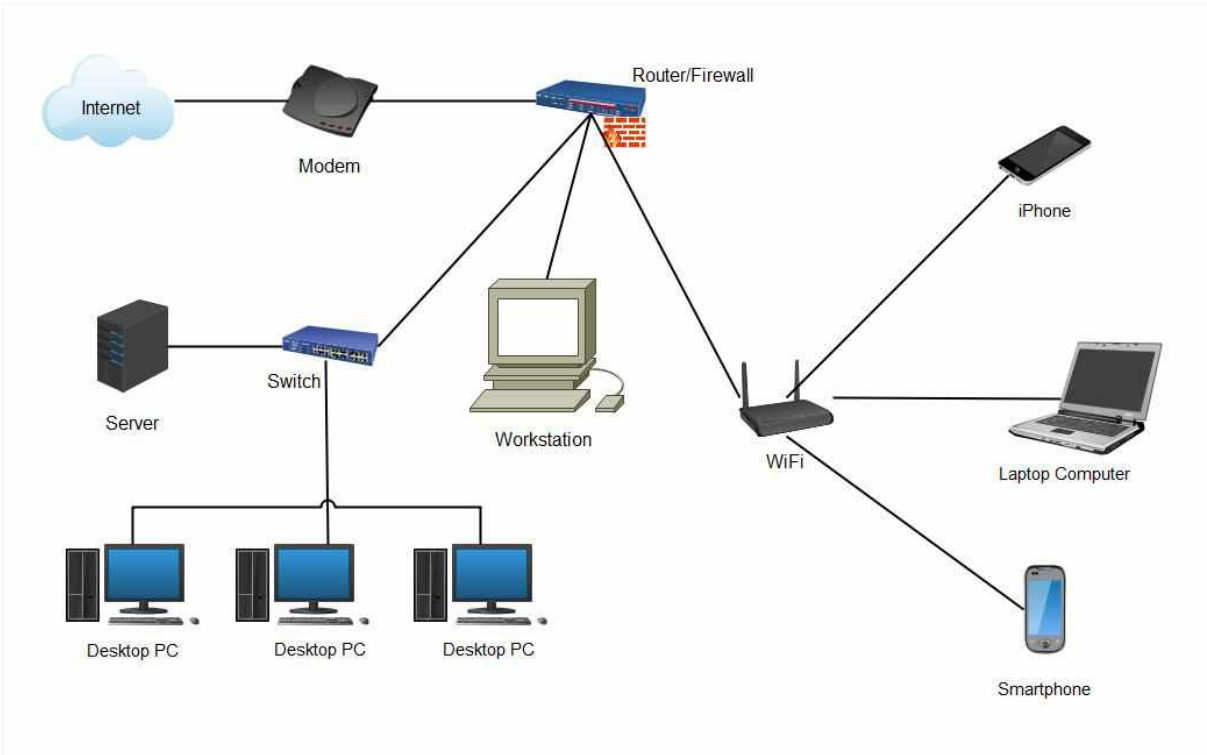
1) What is the definition of a network in IT/communication systems?
2 or more devices connected together that can communicate, possibly share files etc

2) What is a PAN, LAN, MAN & WAN - give an example of where each might be used?
PAN: personal area network - e.g. Bluetooth connection between phone & PC/headphones
LAN: local area network - e.g. home/office/classroom network with various devices
MAN: metropolitan area network - e.g. city-wide WiFi or university network across multiple campuses in the same city
WAN: wide-area network - e.g. entire Internet, company network that allows employees to access files, send internal emails between offices in different cities/countries

3) Draw a diagram of a LAN with several devices connected to it

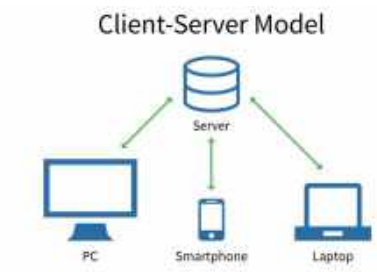


Note: the modem & Internet aren't part of the LAN - they are just showing how a LAN could be connected to the Internet (though LANs can also be air-gapped (not connected) to the Internet too)

4) What is the client-server model - draw a quick diagram demonstrating it

Client: a device that sends a request
Server: a device that fulfills that request

So this is the client-server model – simply that a client requests something and a server fulfills that request. Communication will occur according to a given protocol (e.g. HTTP(S), FTP(S), SSH etc)



5) What is a thin-client & what is a thick-client - what are some advantages/disadvantages of each?

Thin-client: all/most processing done on server; client is simply an I/O system (keyboard/mouse/screen) etc to interact with the system. Advantages:

- Host software on server, hence only need one license = cheaper
- Less storage requirements - one copy needed; clients don't need to have copies of the software/data
- Reduce energy usage
- Updates/management/monitoring/setup is easier/quicker - only have to be applied to one machine (server)
- Less downtime - since only one copy of software/configurations/data etc, there should be less problems than if each user has and can potentially mess up their own software
- Possibly more secure - only one attack point, rather than each
- Can't copy data to own device (e.g. employees copying and selling their own company's intellectual property/blackmail)
- Can access remotely if they can connect to the server

Thick-client: all/most processing done on the client; server does little/no processing. Advantages:

- Reduces load (hence financial cost) on servers - particularly true if users aren't from within company (e.g. users of a website) - it's better if they do the processing in their browser, in terms of saving server costs/ensuring the servers don't get overwhelmed with requests/even targetted DDoS attacks on resource-heavy processes
- Quicker - user does processing on their device, without having to wait for data to be sent to and from the server
- Greater customisability - user probably has more permissions/options when modifying software/files on an individual device, rather than the central server
- Easier for developers to create complex programs & GUIs that run locally, rather than central server

6) List some advantages and disadvantages for both the client-server and peer-to-peer model

Client-server:
If file is available, then the whole file is available
Easy to setup/manage (add, delete, rename, copy etc) files, since they're all stored in one place
Less viruses - i.e. if downloading from a reputable company, you can be fairly sure the download will be safe
User doesn't require additional software to download files (like they do with p2p)

Peer-to-peer:

Can be faster, since you can download parts of the file from different seeders (users/peers) simultaneously
Can be multiple copies of same file, so resistant to server malfunctions, original file not becoming available (e.g. if company goes bankrupt), police takedowns etc
More anonymized (private) for downloaders (leechers)
Cheaper for creator of files - resources/hardware is offloaded to others, they don't need huge numbers/amounts of servers/storage themselves

7) What are the 5 requirements for a communication system to function?
Sender, receive, message, communication medium, protocol

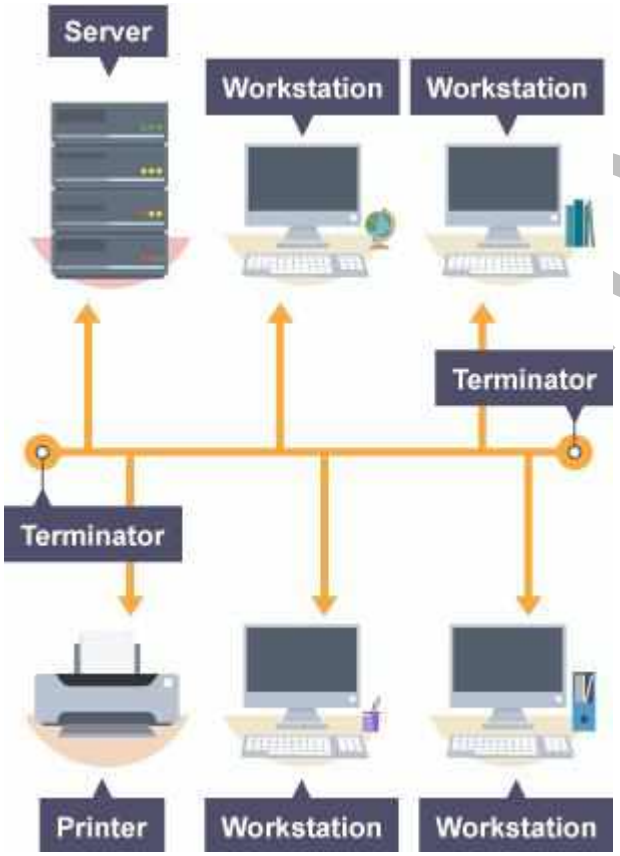
8) There are 6 terms you are required to know - they are: simplex, half-duplex & full-duplex and unicast, multicast & broadcast - give a simple definition of each term

9) List the 4 network topologies required for A-Level and draw a simple diagram of each & try to list at least 2 advantages & disadvantages for each

Point to point:

- Secure – eavesdropping is hard/impossible, hence can connect critical/specialist servers together – e.g. database and file server generating financial reports in a bank
- Fast & reliable – dedicated connection, hence no collisions/lower congestion etc

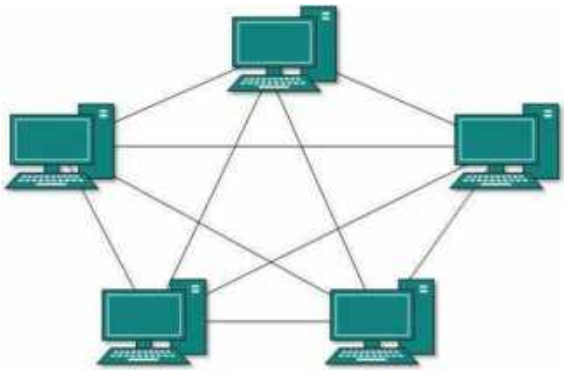
- Not general purpose – can only connect two devices
- No redundancy – single point of failure
- Expensive – need dedicated connection between device

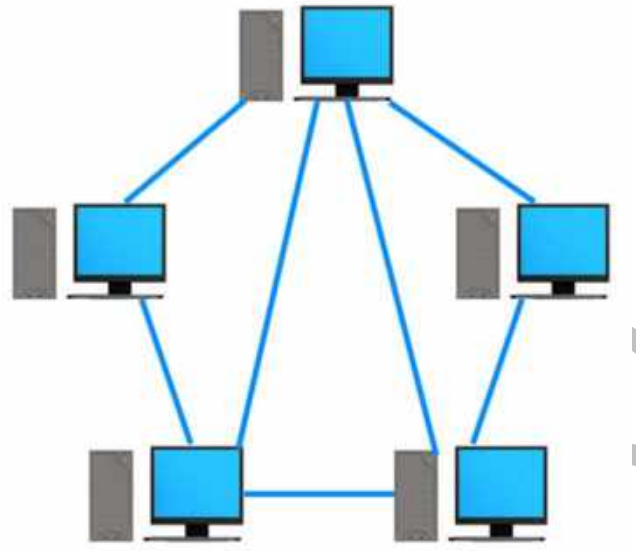


- Semi-resilient - a fault in a node or a link connecting a node to a bus won't prevent communication between other nodes
- Relatively easy to implement
- Efficient for small networks
- Less network cable/cheaper e.g. star/mesh networks
- Easy to expand – simply add device to existing line

- Slow for large networks, since each additional device slows network down
- Potential for eavesdropping, since data intended for a particular client is broadcast along public bus
- Identification of problem difficult if there's a fault in the line (as opposed to e.g. star topologies, where the specific problem link can be identified)
- Chance of collisions – hence packet loss is high

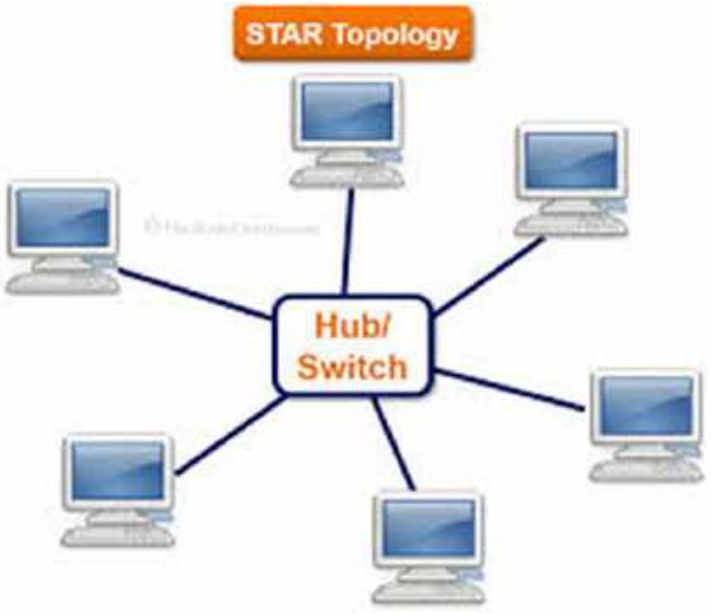
Full & partial mesh:





- Offers full-duplex communication
- Offers all 3 transmission types: unicast, multicast & broadcast
- Supports high traffic load, since multiple devices can transmit data simultaneously across different wires
- Resilient: failure of one line only causes that particular line to go down – other routes can then be used
- High privacy & security due to dedicated connections
- Adding additional devices doesn't disrupt data transmission between current devices
- Fault identification is easy (since you know exactly what line is down)
- No centralized authority

- Expensive/infeasible, due to large amount of wiring
- Building & maintaining is extremely difficult even with a relatively small number of devices
- High power consumption
- Could have redundant connections, even if a partial mesh is used



- Offers full-duplex communication
- Offers all 3 transmission types: unicast, multicast & broadcast
- Due to hub-nodes having point-to-point communications, there are no collisions
- Each device only needs one I/O port to connect to switch
- Relatively easy to implement
- Easy to identify fault, due to point-to-point links
- Resilient due to point to point links (unless central hub goes down)

- If central switch/hub fails, the whole network fails
- More expensive/more cable than bus…but less than full/partial mesh
- Switch can be under high load in large network
- Extra hardware (switch/hub) required compared to bus topology
- Performance depends on the switch (specs, throughput, load etc)

10) Define the following terms:

Bandwidth: the amount of data that can be sent over a network per unit time - e.g. 100Mb/s, 50GB/month etc

Attenuation: the effect of the signal strength decreasing over distance travelled

Interference: when multiple signals/electromagnetic waves exist simultaneously, they will create a resulting waveform that is a combination of all of them, hence corrupting data/losing the original waves

Channel: a distinct frequency band that signals can be sent over - e.g. radio waves in WiFi/mobile networks, light pulses in fibre optic etc

11) Name as many wired and wireless transmission mediums as you can

Wired: twisted pair, coaxial, fibre optic
Wireless: WiFi, satellites, bluetooth

12) Complete the table:

Type	Advantages	Disadvantages
Coaxial	Moderate price/bandwidth/interference/attenuation/need for repeaters	
Twisted pair		Lower bandwidth & more

	Cheap	interference/attenuation/need for repeaters than other wired approaches
Fibre optic	Extremely high bandwidth, low attenuation/need for repeaters, not affected by interference that much	Expensive, requires specialist equipment to use
WiFi	Convenient/portable/no wires, easy to connect, cheap	Low bandwidth, potential for eavesdropping
Satellites	Can use in remote locations & after natural disasters	Extremely expensive, difficult to create, low bandwidth (1 satellite shared between 100000+s of users)

13) A company has a site spanning 4km^2 - they have 4 buildings (office, factory, distribution center, research), each about 500m apart - in each building, they might have multiple networks, but a network will never have more than 10 computers - in total, the company has about 500 computers - suggest & justify a topology/ies they could use as well as an/some appropriate transmission medium(s)

A full or partial mesh network could be used to connect the 4 buildings - this provides fast, secure and reliable communication due to the possibility for rerouting via another node in the mesh if one of the routes becomes unavailable. Either coaxial or fibre optic could be used to connect the 4 buildings, depending on how much bandwidth the company expects to use - fibre optic could support a higher bandwidth, but would be more expensive than coaxial. As for the individual networks in the buildings, they could be connected via a star - this offers high-performance, a fault (unless it's the central switch) won't affect the other devices and communication is secure as other devices will only receives frames/packets that the switch has checked are intended for them. Unicast/multicast/broadcast would also be supported. A star topology is cheaper/requires less wire than a mesh, but offers better performance than e.g. a bus network

14) Complete the following table about network hardware:

Device	Purpose
Terminator	A resistor placed at each end of the bus line to stop electrical signals reflecting back down the line and causing interference
Repeater	Takes incoming signals and retransmits them at their intended full amplitude - this is designed to counteract the reduction of signal intensity due to attenuation
Router	Uses its routing table to determine the next device (hop) to forward/route the packets to
Wireless Access Point (WAP)	Allows devices to wirelessly connect to it - contains an antenna to transmit & receive signals
Hub	Central device in a network that broadcasts all frames/packets to all other devices on the network - rarely used these days
Switch	Central device in a network can send packets via unicast, multicast or broadcast
Bridge	Used to connect two LANs/network segments and join them together, as though they were one network
Gateway	Is the entry/exit point of a network - can convert between and allow networks of different protocols to communicate. Can act as a firewall allowing/blocking incoming/outgoing packets based on a set of criteria
Network Interface Controller/Card (NIC)	Contains Ethernet port, establishes initial connection, communication (buffering, error correction, interrupts), stores MAC address, performs encryption/decryption etc

Wireless Network Interface Controller/Card (WNIC)	as above, but no Ethernet port & supports wireless connections instead

15) A typical home router performs the features of/contains many of these devices listed above - which devices are they? And why is a home router multi-functional?
A home router provides the function of a: router, wireless access point, switch/hub, gateway and bridge. The reason a router is multifunctional is to make it more convenient/cheaper for the customer - no one wants to buy 5 different devices

16) What is the advantage of a switch compared to a hub? What advantage(s) does this have for the network?
Switch supports unicast, multicast or broadcast - this makes the network more secure, since frames are only sent to those devices they are intended for. Additionally, network congestion will be less, hence network performance will be better, since messages aren't constantly broadcast to devices they're not intended for

17) What is a collision - can they occur on the star or mesh topologies - why or why not?
A collision occurs when two devices send a signal simultaneously and when these signals meet, they interfere with each other, corrupting both - collisions can occur on bus topologies, wireless networks etc (though different channels and other techniques are used to mitigate against this). A collision can't occur on a star or mesh - this is since there are dedicated, usually full-duplex lines for communication unlike the shared bus line

18) How does CSMA/CD (Carrier Sense Multiple Access with Collision Detection) handle collisions on a bus topology?
- Check voltage level on wire (no voltage = no activity)
- If there is voltage (i.e. message), then wait random time before re-checking
- If no activity detected, start transmission
- Continuously check for collision
- If no collision, continue transmission
- If collision, stop transmission & transmit jamming signal to notify other nodes of collision – wait random time and try again

19) 5G uses higher frequency waves than 4G. This means the bandwidth is higher. 5G is worse at going through walls and has a higher rate of attenuation.

20) State the advantages/disadvantages for both wired & wireless communication.

Wireless: portable devices/remote locations, convenient, easy to setup, lower bandwidth, less secure
Wired: higher bandwidth, more secure, requires additional hardware (cables)

21) Define the terms:

WWW: World Wide Web – a collection of webpages linked together and accessed via the HTTP(S) protocol

Internet: inter-network – the worldwide connection of devices and infrastructure (cabling, satellites, routers etc) – communicates over IP and any digital data can be sent – webpages, media, emails, files, programs, text etc

ISP: Internet Service Providers are a company or organization that provids users with access to the internet - i.e. the company you pay your monthly Internet/mobile bill to

22) What are the 3 tiers of ISPs - how does the area they cover differ?

Access/Tier 3 ISPs: allow an individual/business to connect to regional ISP
Regional/Tier 2 ISPs: connect local access ISPs & provide national/regional coverage
Global/Tier 1 ISPs: provide global backbone (undersea cables, satellites etc)

23) What is a buffer and why do network devices - routers, (W)NICs, switches etc need them?

A buffer is a temporary storage space to hold data, as other data is being processed/transmitted. They allow devices operating at different speeds to communicate (since the data can be temporarily held while waiting for the other device to become available/finish processing), storing packets until all have arrived when they can be reordered etc

24) Explain the basic operation of circuit switching and packet-switching approaches for transmitting data - what are the advantages/disadvantages of each?

Packet switching operation:
Data is sent without a connection being established between the sender & receiver – this means establishing the connection is fast, but the receiver may be unreachable – device off, network error etc
Routers forward packets onto the next hop based on their routing table
Data – say an image – will be split into many smaller packets (usually not larger than 1460 bytes) – packets may travel different routes or arrive out of order – they will then be re-ordered at the destination (if using TCP)

Packet switching advantages/disadvantages:

- Doesn't require dedicated infrastructure for each user – many people can share the same e.g. fibre optic cables – cheaper and more scalable
- As such, there's a better utilisation of hardware
- Can be faster – packets can be sent along the faster route (hopefully)
- No connection required (connectionless) – lower initial delay (latency)
- Reliability can be built-on top – e.g. a higher level protocol like TCP which will resend packets that don't arrive and reorder them upon arrival

- Packet loss – some packets might not arrive at destination (misconfigured network, broken router/cabling, full buffers)
- Packets can arrive in wrong order
- Variable latency – packets travelling different routes will take different time – might have to wait for all to arrive to reassemble
- Header overhead – small amount of extra data needed in every packet header (source & destination IP, packet length, version 4/6, checksum, time-to-live (TTL) etc)

Some of these issues can be handled though – for example, rerouting & higher-level protocols like TCP helps to ensure all packets should arrive

Circuit switching:
A physical link between sender & receiver is required – this could be with someone on the other side of the world
Connection must be established before communication can begin
Channel is dedicated for only those 2 users for duration of communication

Ensures receiver is reachable before sending
Dedicated channel required (can be an advantage (reliable, high bandwidth) or disadvantage (wasteful))
Suitable for long, continuous communication (e.g. phone calls)
Data will arrive in correct order

System has many backup generators – you can still make phone calls in an emergency (e.g. calling emergency services in a flood

If all channels being used, you won't be able to connect
Higher cost (due to requirement of dedicated channels)
Higher initial latency due to ensuring receiver is available

25) What is/was the PSTN (Public Switched Telephone Network) system and why were 'leased lines' sometimes required?

The PSTN is the collection of telephone communication infrastructure (telephone lines, switches, exchanges etc) that had been available in many countries for 100+ years - when the Internet was gaining popularity, the millions of km of underground/undersea fibre-optic wires we have today didn't exist, hence existing infrastructure had to be used. The problem was that a line could only be used by 2 people at once (sender and receiver) - hence there were often times when people wouldn't be able to access the Internet since all the lines were in use. For large companies, governments, military, hospitals etc not being able to connect wasn't practical - hence they would rent their own private line (a "leased line") that could only be used by them - giving them 24/7 access

26) What is cloud computing & what is the difference between a private & public cloud? What would some general advantages/disadvantages of cloud computing and public/private clouds in particular?

Cloud computing is the provisioning of computing services via the Internet

Clouds can be either private within the company or public like (AWS, Baidu, Azure, Alibaba, Tencent, Google etc). For the private cloud option, there are 3 choices

Organisation creates and manages their own on-site cloud
Organisation outsources to a 3rd party to create & manage on-site cloud
Organisation outsources to a 3rd party to create & manage off-site cloud

For public clouds - there is only one scenario - your data/websites/processes are hosted in a data center operated by another company in a different (remote) location

General cloud computing advantages:
Remote access – employees can access files from anywhere

Collaboration – employees can work on same files simultaneously

Can be used as a remote backup

Big cloud company might have better security than a system we could make ourselves

"Reduces complexity" if a public cloud – someone else handles it

General cloud computing disadvantages:
[Mostly public cloud] You are storing your data with another company – you have to trust them & their security/privacy standards

MUCH more expensive than traditional servers [Private cloud would be more expensive initially, but cheaper than public cloud if operating at large scale/for a long time]

Some software can't be run as effectively when distributed across multiple servers (e.g. databases)

[Public cloud] Less customisable/control compared to having your own servers

27) What kinds of services might a cloud company provide (hint: IaaS, PaaS & SaaS)

Infrastructure as a Service: cloud compute/GPU renting etc

Platform as a Service: application hosting where OS/security/updates etc are handled by cloud provider

Software as a Service: file backup/sync, online office tools/IDEs, Github, online email, Grammarly etc

28) What is a routing table and why is it needed to correctly route packets to their destinations?

A routing table is a data structured used to determine the next device (hop) an incoming packet should be sent to - example data included in the routing table could be IP ranges, the IP of the potential hop, the physical port it's connected to, metrics/heuristics/status details about particular hops. These details are required to ensure efficient and reliable routing of packets over the Internet

29) What is bit-streaming and what are the differences between on-demand and realtime bit-streaming?

Bit streaming is the process of a device accessing a continous flow of data from another source.
On-demand:

- streaming from a source that already exists.
- Media files stored on server and converted to a streaming format
- Can pause, rewind, fast-forward etc
- Often better quality – buffering makes short connection drops less of an issue

Realtime:

- streaming from a live source
- Event is captured in real-time and live media sent
- (Might not) be saved on server – hence, once it's been sent out, it has "gone" and can't be rewatched, paused etc. Packet loss over UDP can be an issue – parts of video/audio will be lost

30) What are the high and low watermark levels in bit streaming?

High-watermark: level at which streaming software (e.g. media player) will tell the media server to stop sending data, since the buffer is nearly full

Low-watermark: level at which streaming software will tell the media server to resume sending data, since the buffer is nearly empty

31) How many IP addresses are available in IPv4 - why is this a problem?

2^{32} = 4,294,967,296 (4.3 billion) - yet there are more than 8 billion people in the world, many people have multiple devices etc, so this is not enough unique IP addresses

32) Explain the similarities and differences between IPv4 and IPv6 addresses and formats

Similarities:
- both can be public & private
- dynamic or static
- split into groups with a separator

- support subnetting
- uniquely identify a device on a network

Differences:
- IPv4 uses 32 bits, IPv6 used 128 bits - IPv6 hence has far more possible addresses
- IPv4 uses 4 groups written as 8-bit denary values in range 0-255, IPv6 groups are written as 8 groups of hexadecimal digits in range 0000-FFFF
- IPv4 uses a dot separator "." - IPv6 uses colon ":"
- IPv6 can be dual IPv4 & IPv6 addresses (for backwards compatibility)
- IPv6 has a more complex packet header

33) Write whether the following IP addresses are valid or invalid - give a reason if invalid:

192.168.0.1 - valid
50.256.48.14 - invalid (256 > maximum allowed group value of 255)
70.25.1.5.12 invalid (IPv4 should have 4 groups)
2001:DB8:3333::ADBE:7777:8888 - valid
:: - valid (IPv6 address of all 0s)
2001:db8::123.123.123.123 - valid (dual IPv6 and IPv4 address)
1234:5678:9876:ABCD:DEFE:1357:2468 - invalid (7 groups and no repeated groups of 0s denoted by "::" - should be 8 groups for IPv6)
DEAD:FACE::EAT::BAD:F00D - invalid (can't have multiple repeating groups of 0 denoted by "::")
75.148:182.92 - invalid - IPv4 should use "." separator, not ":"
G00D:C0FF:EE:: - invalid ("G" isn't valid hexadecimal character)
AAAA:BBBB::1111.222 - valid

34) What are 3 approaches used to alleviate the IPv4 shortage?

Subnetting
Private IPs
Dynamic IPs

Or just create a complete new format - IPv6

35) List 3 benefits of splitting a network into subnets

- Allows greater utilisation of IP space – i.e. less wasted IP addresses
- Makes networks easier to organise & maintain for large networks – though does require initial expertise to setup
- Improves security – i.e. different firewall rules/levels of security based on the subnet
- Network separation: different departments (e.g. finance and research) don't have access to other network/files. Hackers/malware can also (hopefully) be contained to single subnet
- Improves efficiency by breaking down big, busy networks – this however does make it slightly more expensive, since additional routers are required (though for a company, this cost is insignificant)

36) What is a subnet mask - explain what a subnet mask of 255.255.255.0 means for an IPv4 address of 200.150.100.1. How many devices would be able to be on this network?

A subnet mask is used to split an IP address into two parts - a network ID and a host (device) ID. A bit value of 1 in the subnet mask (255.255.255.0 = 11111111.11111111.11111111.00000000) means the corresponding IP bit represents the network, while a subnet mask value of 0 means the corresponding bit in the IP address represents the host - i.e. with the subnet mask 255.255.255.0, we have 24 1s, then 0s - hence using the above IP address, the network part is 200.150.100, while the host ID is 1. Since we have 8 bits allocated for the host IDs, that means the subnet can support 2^8 = 256 different devices

37) What is Network Address Translation (NAT)?
NAT is used to allow multiple devices on a local area network to be globally accessible by the same public IP. NAT is hence responsible to translating between private and public IP addresses - in practice - the devices on the LAN will have a private IP like 192.168.0.1, while when communicating over the Internet, the router will set outgoing packets to have its publicly-accessible source IP address, hence allowing the packets to successfully arrive back in that router in the response - the router will then be responsible for forwarding these packets onto the correct device on the network based on its NAT table

38) Explain the difference between static & dynamic IP addresses - what are the advantages/disadvantages of each?

Static IP - fixed, doesn't change unless user specifically changes it themselves
Suitable for servers - don't want IP to constantly change, since clients/software won't know where to send packets to
More trustworthy - companies are less likely to engge in malicious behaviour if having a fixed presence on the Internet
Less private - activity can be tracked more easily if IP is fixed
More expensive due to renting the IP permanantly (and there being a limited supply)

Dynamic IP - allocated by DHCP server (private IP will be allocated by DHCP server in home router - router's public IP will be allocated by ISP's DHCP server) - IP can change periodically, if device is switched off then on again etc

Alleviates IPv4 shortage - if a device isn't using an IP address, it can be assigned to another device
More private - harder to track user's activity if their IP is regularly changing
Cheaper
Not suitable for many servers - e.g. don't want web/email server to constantly change IP address, since packets won't arrive at correct server, new DNS requests will have to be sent to find new IP etc

39) Explain the difference between public & private IP addresses - what are the advantages/disadvantages of each?

Public IPs are unique and globally accessible from any other device on the Internet - in contrast, private IPs fall in designated fixed private IP ranges (e.g. 192.168.n.n/16). Private IP addresses can be reached from other devices on the LAN, but not from devices outside the LAN - NAT would be required to communicate between private devices and devices on other networks

Public IP:
Globally accessible
Direct communication
Simpler - NAT not required
Privacy/security risks - IP is visble to anyone
More expensive (due to limited supply, especially if static)

Private IPs:
Alleviates IPv4 shortage - only the router needs a public IP address, not each device on the network
Security/privacy - people outside the network will see your router's public IP, not your device's IP
Cheaper - only have to rent 1 dynamic IP from your ISP (allocated to your router by the ISP's DHCP server)
More complex setup/requires NAT

40) What is DHCP and how does the DHCP lease work?

Dynamic Host Control Protocol - responsible for automatically assigning dynamic IPs to devices when a device requests one (i.e. when it tries to connect to network). A device will ask the DHCP server for an IP and the DHCP server will grant them one for a period of time – usually, this will be between 1 hour to 1 week (let's assume 8 hours, to make the maths easier)

When half the lease time has passed, if the device is still online, it will ask the DHCP server if it can extend the lease

If the DHCP server is unavailable, the requesting device will wait half the time and try again – e.g. if the initial lease is 8 hours, the device will wait the following time to try and renew the lease: 4 hours 2 hours 1 hour 30 minutes 15 minutes 7.5 minutes etc…if not renewed in time, the IP will become available for another device

41) Explain what DNS is used for and how it works

Domain Name System - resolves (maps) human-readable domain names (like example.com) that are easy for humans to remember to IP address which are used when two devices communicate on a network (like a client sending an HTTP request to a web server). Effectively it's a key-value store database mapping domain names to IP addresses, like an old phone book

DNS is hierarchical – a DNS record will be looked for in these places – if it's not found, it will be looked for in the next layer.

Browser & operating system
Router's DNS server (cache)
ISPs DNS server
Root -> top-level domain server -> authoritative name server

DNS records will be cached to avoid overloading DNS servers with requests for already visited websites - this will also reduce latency for the user, since the DNS request won't have to be performed before the HTTP(S) request each time

42) Why is it important for DNS records to be cached - what could be a problem of the records being cached too long however?

DNS records will be cached to avoid overloading DNS servers with requests for already visited websites - this will also reduce latency for the user, since the DNS request won't have to be performed before the HTTP(S) request each time

If DNS records are cached too long, they could expire/become invalid if a website changes its IP address (e.g. if moving to a new server, network reconfiguration etc). There is also the security risk of DNS cache poisoning - this is when DNS requests have been intercepted by a malicious third party and a fake IP has been returned

(e.g. of a spoofed website as part of a pharming attempt) - if this DNS record is kept indefinitely, the user will always be redirected to this fake site, without them knowing.