

Communication

A-Level Computer Science 9618 · Topic 2 revision notes

Everything from the 6 lessons of this topic on a few pages: the key idea of each lesson, the diagram to remember, the points to learn and the traps examiners set. Read it, cover it, test yourself.

1. LANs, WANs, client-server and peer-to-peer

2. Network topologies and hardware

3. Cloud computing

4. Wired and wireless media, Ethernet and CSMA/CD

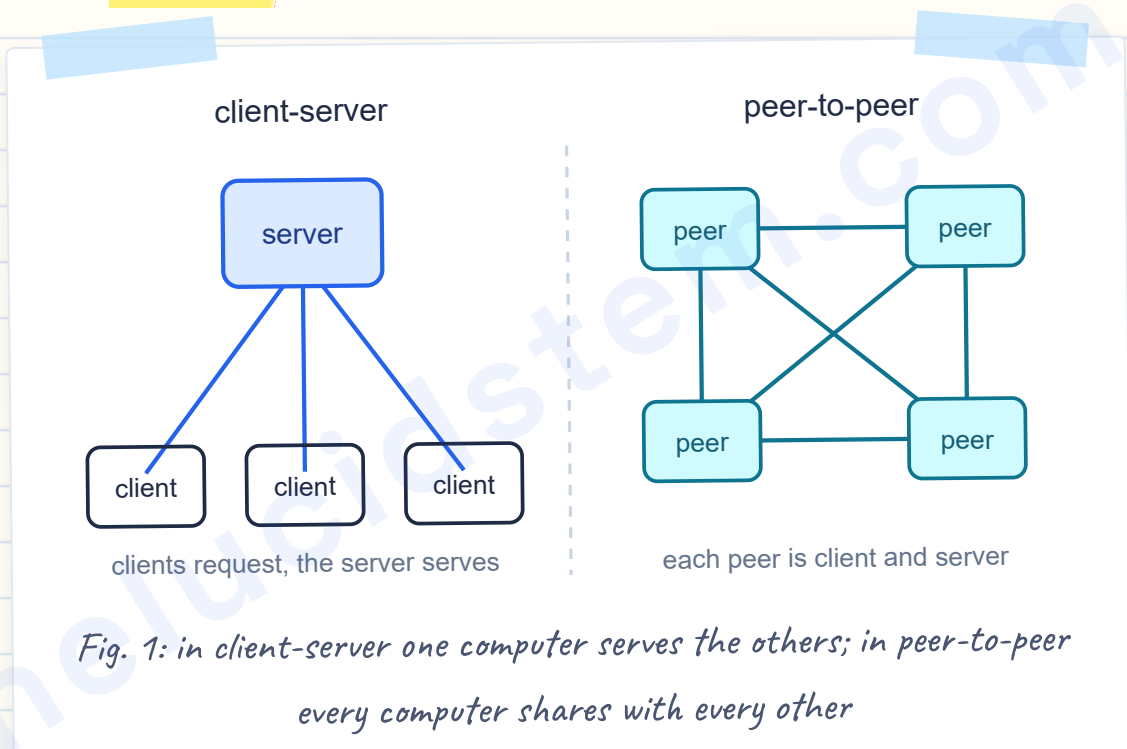
5. The internet and the world wide web

6. IP addressing and the domain name service

1 LANs, WANs, client-server and peer-to-peer

Syllabus 2.1

A **network** lets devices share resources, data and communication. A **LAN** covers a small area (one site) and its infrastructure is owned by the organisation; a **WAN** covers a large geographical area and uses infrastructure such as telephone lines and satellites leased from others. In the **client-server** model, clients send requests to a central **server** that provides a service and holds the data. In the **peer-to-peer** model there is no central server; every **peer** is both a client and a server. A **thin client** depends on the server for processing and storage; a **thick client** does most of its own processing.



Worked example: Justify a model

A dental practice has 6 computers. Patient records must be kept secure, backed up every night and opened by any receptionist from any desk. Recommend a model and justify it.

1. Pick out the requirements: security, nightly backup, access to the same records from any computer.
2. Client-server holds the records centrally on the server, so one backup covers everything.
3. Access rights and log-ons are controlled centrally, which keeps the records secure.
4. Users log on from any client and see the same, up-to-date records.

Answer: Client-server, because the records are stored, secured and backed up centrally and are available from any client

Roles decide the model.

- ✓ **LAN vs WAN:** area covered and who owns the infrastructure.
- ✓ **Client-server:** central server provides services; central security and backup; single point of failure.
- ✓ **Peer-to-peer:** every peer is client and server; cheap and simple; no central control.
- ✓ **Thin vs thick:** where the processing and storage happen, and whether it works offline.

Watch out!

"A WAN is a big LAN" earns nothing. Give the defining differences: geographical area covered, and who owns the infrastructure (a LAN's is owned by the organisation; a WAN uses leased or public communication links).

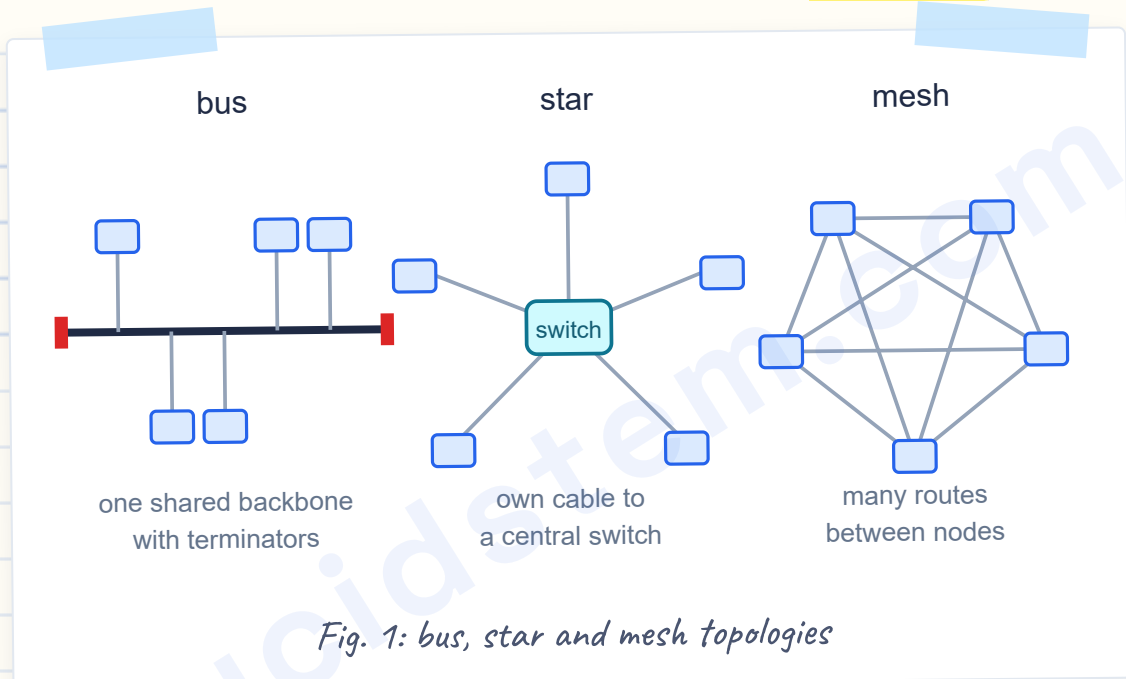
Always tie a justification to the scenario. "Client-server is more secure" is weak; "the patient records are on one server, so access rights and backups are managed centrally" earns the mark.

Thin and thick describe the *client*, not the server, and both still exist inside a client-server network. A thin client is not "a client with a slow connection".

2 Network topologies and hardware

Syllabus 2.1

In a **bus** topology every device shares one backbone cable, so every packet reaches every device. In a **star** each device has its own cable to a central **switch**, which sends each packet only to its destination. In a **mesh** devices are linked to several others, so packets can take more than one route. A **hybrid** combines two or more topologies. A LAN is built from **NICs/WNICs**, **cables**, **switches**, **WAPs**, **servers**, **bridges** and **repeaters**; a **router** connects the LAN to other networks and forwards packets using **IP addresses**.



Worked example: Justify a topology

A hospital network must keep working even if one cable or one device fails, because patient monitors send data continuously. Which topology should it use?

1. Identify the requirement: no single point of failure.
2. A bus fails if the backbone breaks; a star fails if the switch fails.
3. A mesh has several routes between nodes, so packets can be re-routed round a failed cable or device.

Answer: Mesh (or a hybrid with a mesh core), because there is more than one route between devices

Follow the packet.

- ✓ **Bus:** every device sees every packet; one backbone, terminators, one break stops all.
- ✓ **Star:** switch forwards only to the destination; the switch is the single point of failure.
- ✓ **Mesh:** many routes, no single point of failure, expensive.
- ✓ **Switch vs router:** MAC within a network vs IP between networks.

Watch out!

A mesh is not "every computer connected to every other" by definition; that is a *full* mesh. A partial mesh, like the internet's core, still gives several routes between nodes.

Do not mix up a switch and a router. A switch works *within* one network and uses MAC addresses; a router works *between* networks and uses IP addresses.

thelucidstem.com

3 Cloud computing

Syllabus 2.1

Cloud computing is the delivery of computing services (storage, processing power, software and platforms) on demand, over the internet, from remote servers in data centres. A **public cloud** is run by a provider and its servers are shared by many organisations and members of the public, who pay for what they use. A **private cloud** is used by a single organisation, either on its own premises or hosted for it, giving more control and security. Benefits include **access from anywhere**, **scalability** and **no hardware to maintain**; drawbacks include **dependence on the internet connection**, **security and privacy concerns** and **loss of control** over the data.

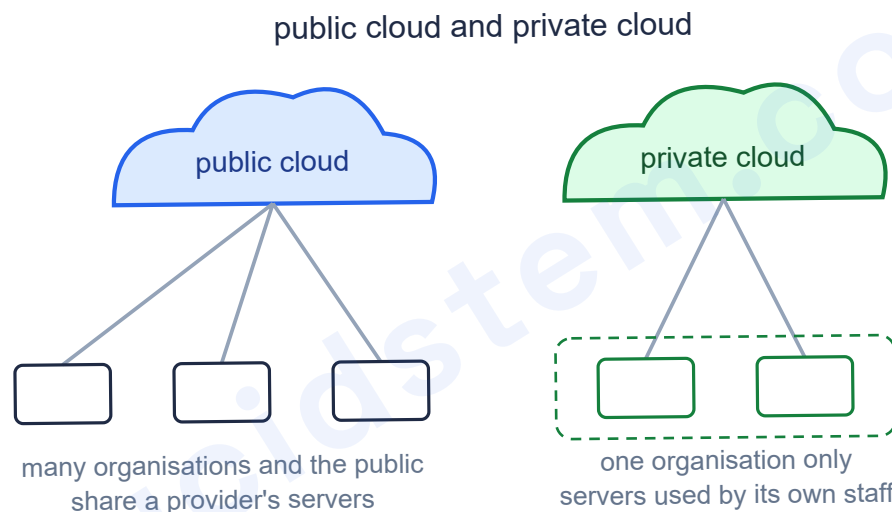


Fig. 1: a public cloud is shared by many users; a private cloud serves one organisation

Worked example: Weigh it up

A small architecture firm of 8 staff is deciding whether to store its drawings in a public cloud. Give one benefit and one drawback, each in context.

1. Benefit: staff can open the drawings on site visits from any device with an internet connection.
2. The firm does not need to buy a file server or employ a technician, because the provider maintains the hardware and backups.
3. Drawback: if the office internet connection fails, staff cannot open the drawings they need.
4. The drawings are confidential client work held by a third party, so there is a risk of unauthorised access.

Answer: Access from anywhere with no hardware to maintain, against dependence on the internet and the security of a third party

Always in context.

- ✓ **Cloud:** remote servers, reached over the internet, providing storage, software and processing.
- ✓ **Public:** shared provider servers, pay per use, less control.
- ✓ **Private:** one organisation, more control and security, more expensive.
- ✓ **Evaluate:** pair each benefit with a drawback and tie both to the scenario.

Watch out!

Cloud storage is not the same as a local file server. The data is held off-site by a third party and reached over the internet, which is exactly why the benefits and drawbacks differ.

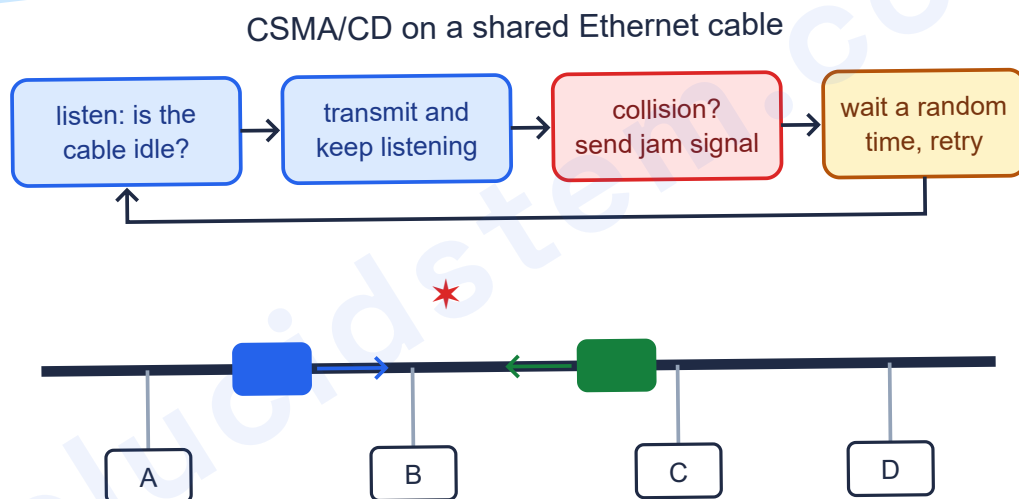
"Cloud is cheaper" is only true for start-up costs. Over many years the subscription can cost more than owning the hardware, so qualify the claim.

4 Wired and wireless media, Ethernet and CSMA/CD

Syllabus 2.1

Copper cable (twisted pair or coaxial) carries electrical signals: cheap and easy to install, but it suffers from **interference** and **attenuation**. **Fibre-optic cable** carries pulses of light: very high bandwidth over long distances, immune to electrical interference, but more expensive. Wireless media (**radio waves** including WiFi, **microwaves**, **satellites**) give mobility without cables but are slower, less secure and more affected by interference.

Ethernet is the standard protocol for wired LANs; on a shared cable it uses **CSMA/CD**: listen before transmitting, detect any collision, send a jam signal, then wait a **random time** before trying again.



A and C both sense an idle cable and send: their frames collide

Fig. 1: CSMA/CD: listen, transmit, detect a collision, jam, back off for a random time and retry

Worked example: Why random?

Explain why each device waits a random time after a collision rather than a fixed time.

1. Both devices detected the same collision at the same moment.
2. If they each waited the same fixed time, they would sense the cable idle together and transmit together again.
3. A random wait makes it likely one device starts first; the other then senses the cable is busy and waits.

Answer: So the two devices do not retransmit at the same moment and collide again

Four headings.

- ✓ **Compare media by:** bandwidth, distance (attenuation), interference, cost.
- ✓ **Wireless:** mobility and easy set-up against interception, interference and lower speed.
- ✓ **CSMA/CD:** listen, transmit, detect collision, jam signal, random wait, retry.
- ✓ **Avoidance:** switches with full-duplex links stop collisions happening.

Watch out!

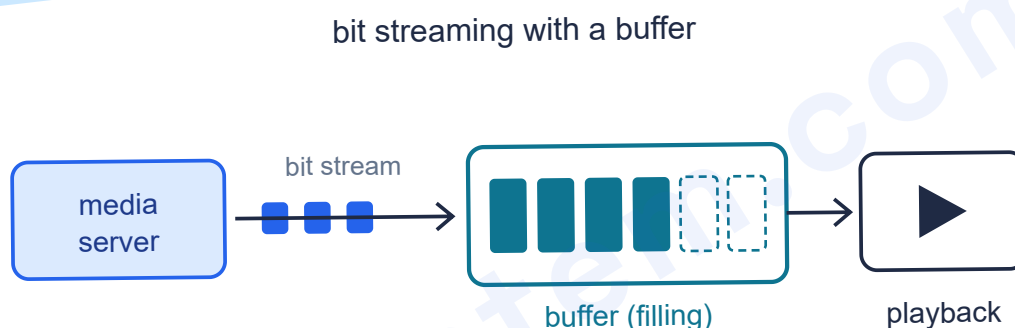
Wireless is not insecure by nature, but its signals spread beyond the building. The mark is for saying that signals can be intercepted, so data must be encrypted.

CSMA/CD does not prevent every collision: it detects them and recovers. Make sure the answer includes the jam signal and the random wait, which are the commonly missed marks.

5 The internet and the world wide web

Syllabus 2.1

The **internet** is the global **network of interconnected networks**; the physical infrastructure of cables, routers and links. The **World Wide Web** is a **collection of web pages and resources**, linked by hyperlinks and reached using HTTP(S) and a browser; it is just one service that runs over the internet. The internet is supported by **modems**, the **PSTN**, **dedicated lines** and the **cell phone network**. **Bit streaming** sends audio or video as a continuous stream of bits that is played as it arrives, from a **buffer**, either **real-time** (live) or **on-demand** (pre-recorded); the connection's **bit rate** must be at least the stream's bit rate.



data arrives at the bit rate of the connection; it is played from the buffer if the buffer empties because the connection is too slow, playback pauses

Fig. 1: a streamed file is played from a buffer while the rest of it is still arriving

Worked example: Data used by a stream

A film is streamed at 5 Mbps for 1 hour. How much data is transferred, in gigabytes? (1 Mbps = 1 000 000 bits per second; 1 GB = 1 000 000 000 bytes.)

1. Bits per second: 5 000 000.
2. Seconds in an hour: $60 \times 60 = 3600$.
3. Total bits: $5\,000\,000 \times 3600 = 18\,000\,000\,000$ bits.
4. Bytes: $18\,000\,000\,000 \div 8 = 2\,250\,000\,000$ bytes = 2.25 GB.

Answer: 2.25 GB

Hardware versus service.

- ✓ **Internet:** the network of networks (infrastructure). **WWW:** linked web pages, a service over it.
- ✓ **Hardware:** modem, PSTN, dedicated line, cell phone network: say what each does.
- ✓ **Streaming:** played from a buffer as it arrives; real-time (live) or on-demand (stored).
- ✓ **Calculations:** $\text{bits} = \text{bit rate} \times \text{seconds}$; divide by 8 for bytes.

Watch out!

"The internet is the web" and "you use a browser to get on the internet" both lose marks. Email, for example, uses the internet but not the web.

Watch the units: bit rates are in bits per second (lower-case b), file sizes usually in bytes (upper-case B). Divide by 8 to convert bits to bytes.

6 IP addressing and the domain name service

Syllabus 2.1

An **IP address** identifies a device on a network so packets can be routed to it. **IPv4** is **32 bits**, written as four denary numbers 0 to 255 separated by dots; **IPv6** is **128 bits**, written as eight groups of four hex digits separated by colons. **Subnetting** uses a **subnet mask** to split an address into a **network ID** and a **host ID**, dividing one network into smaller ones. A **private** address is used only inside a LAN and is not reachable from the internet; a **public** address is unique on the internet. A **static** address never changes; a **dynamic** one is assigned by **DHCP** each time a device connects. A **URL** names a resource; the **DNS** translates its domain name into the IP address of the server.

IPv4 address AND subnet mask = network address

IP address	192.168.20.77	01 001101 (77)
mask	255.255.255.192	11 000000 (192)
network	192.168.20.64	01 000000 (64)

network ID: 26 bits

host ID: 6 bits

this host is host 13 on subnet 192.168.20.64 (64 addresses: .64 to .127)

Fig. 1: ANDing an address with the subnet mask 255.255.255.192 gives the network address 192.168.20.64

Worked example: Find the network address

A host has IP address 192.168.20.77 and subnet mask 255.255.255.192. Find the network address and the number of usable host addresses in the subnet.

1. The first three octets of the mask are 255, so 192.168.20 is copied unchanged.
2. Last octets in binary: 77 = 01001101 and 192 = 11000000.
3. AND them: 01001101 AND 11000000 = 01000000 = 64. Network address 192.168.20.64.
4. The mask has 26 ones, so 6 host bits: $2^6 = 64$ addresses, minus 2 = 62 usable hosts.

Answer: 192.168.20.64, with 62 usable host addresses

Mask, then AND.

- ✓ **IPv4:** 32 bits, four denary numbers 0 to 255. **IPv6:** 128 bits, eight groups of four hex digits.
- ✓ **Subnetting:** address AND mask = network address; usable hosts = $2^h - 2$.
- ✓ **Private vs public:** LAN only and hidden behind NAT, vs unique and reachable on the internet.
- ✓ **DNS:** domain name to IP address, passed up the DNS hierarchy if not known locally.

Watch out!

An IPv4 number cannot exceed 255, because each part is one byte. An address such as 192.168.1.300 is invalid, and is a favourite in "identify the invalid address" questions.

The number of usable hosts is $2^h - 2$, not 2^h : the network address and the broadcast address cannot be given to a device.

The DNS does not send the web page. It only returns the IP address; the browser then requests the page from the web server itself.