

Communication AS

Read online at pastopic.com/cambridge/computer-science-9618/notes/communication

Last checked 30 September 2026

Read first: [Information representation](#)

© 2026 Pastopic. Free for personal study. Please share the link, not the file.

What you need to know

By the end of this topic you should be able to:

1. **Say why computers are networked** and what the benefits are.
2. **Describe a LAN (local area network) and a WAN (wide area network)** and the differences between them.
3. **Explain the client-server and peer-to-peer models:** roles, benefits and drawbacks, and which suits a situation. Explain **thin** and **thick clients**.
4. **Explain the bus, star, mesh and hybrid topologies**, how packets travel between two hosts in each, and justify a topology for a situation.
5. **Explain cloud computing**, public and private clouds, and the benefits and drawbacks of using the cloud.
6. **Compare wired and wireless networks**, and describe copper cable, fibre-optic cable, radio waves (including WiFi), microwaves and satellites.
7. **Describe the hardware in a LAN:** switch, server, Network Interface Card (NIC), Wireless Network Interface Card (WNIC), Wireless Access Point (WAP), cables, bridge and repeater. Describe the role and functions of a **router**.
8. **Explain Ethernet** and how collisions are detected and avoided with **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection).
9. **Explain bit streaming**, real-time and on-demand, and why the bit rate and broadband speed matter.
10. **Explain the difference between the internet and the World Wide Web (WWW)**, and describe the hardware that supports the internet: modems, the PSTN (Public Switched Telephone Network), dedicated lines and the cell phone network.
11. **Explain how IP addresses are used** on the internet: IPv4 and IPv6 formats, subnetting, how a device gets its address, public and private (and security), static and dynamic.
12. **Explain how a URL (Uniform Resource Locator) finds a resource on the WWW**, and what the DNS (Domain Name Service) does.

Packet and circuit switching and TCP/IP layers are A Level (Paper 3) topics.

Understand it

Why network computers?

A **network** is two or more devices connected so they can exchange data. Networking lets an organisation **share files and data**, **share hardware** (printers, one internet connection) and **software**, **communicate** internally, and **manage centrally**: backups, security and updates are done once for everyone.

LAN and WAN

A **LAN** covers a **small geographical area**, such as one site. The organisation **owns the infrastructure**, so a LAN has a high data transfer rate and is easier to secure. It can be wired, wireless or both.

A **WAN** covers a **large geographical area**, such as offices in several cities. It uses **external infrastructure** owned by others (leased lines, satellites, the internet), so the hardware is **not dedicated** to one organisation; it is slower and harder to secure. The internet is the largest WAN.

Client-server and peer-to-peer

In the **client-server model**, the **server** stores the shared data and software, **receives requests** from clients, **processes** them and **sends back the results**; it also handles security and backups centrally. A **client sends requests** to the server, **waits** for the reply and **displays** it. A web browser is a client. Benefits: central backup and security, one consistent copy of each file, easy to add clients. Drawbacks: servers cost money, and if the server fails every client loses its service.

In the **peer-to-peer (P2P) model** there is **no server**. Every computer has **equal status**: it stores its own files, shares some with the others, and is **responsible for its own security**. It is cheap and simple for a few computers, but:

- **security is weaker**: with no central control, the network is only as secure as its least protected computer;
- there is **no central backup**, so a peer's unbacked-up files are lost to everyone if its disk fails;
- files on a peer that is **switched off** can't be reached, and a peer serving others **slows down**.

P2P is a **model** (who does the work), not a topology. Client-server suits many users with private data needing backups (a school, a bank); P2P suits a few friends sharing files.

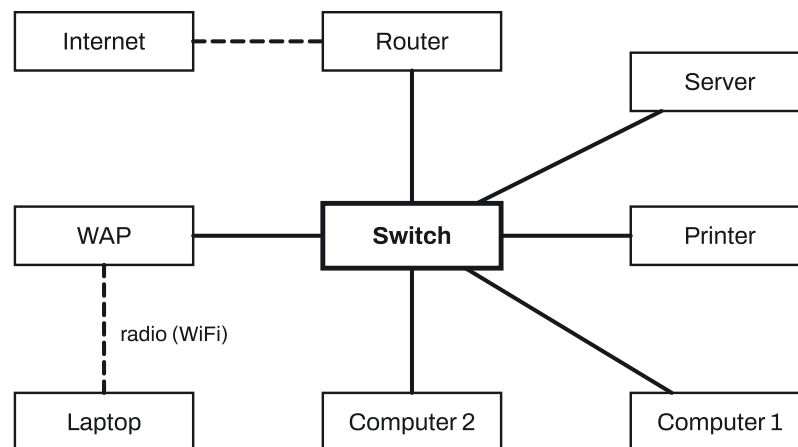
Thin and thick clients describe how much work a client does.

- A **thin client** does very little: the **server does the processing and stores the data**, and the client sends requests and displays results. It needs few local resources but **depends on the server and the network**: if either goes down, it can't work. Software run in a web browser is an example.
- A **thick client does most of its own processing** and holds its software locally; the server does little for it. It copes with a slow network but needs more powerful hardware.

Topologies

A **topology** is the layout of the links between devices (**nodes**, or **hosts** for computers).

Star. Every device has its own cable to one **central device**, usually a **switch** (a router in a small home network), and to nothing else.



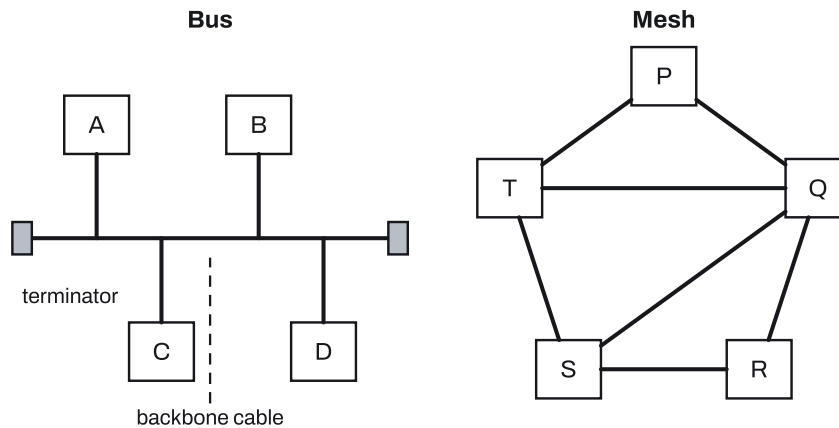
How packets travel between two hosts in a star:

1. The sending computer sends the packet along its cable to the **switch**.
2. The switch reads the packet's **destination address** and looks it up in its table of the devices attached to each port.
3. The switch forwards the packet **only** to the port of the intended device, so no other computer receives it.

A broken cable affects only one device, collisions are rare, and devices are easy to add, but if the switch fails the whole star stops.

Bus. Every device joins **one shared main cable** (the backbone), with a **terminator** at each end. A packet travels the whole cable, so **every device receives it** and only the addressee keeps it. Only one device can send at a time, so a bus has the **most collisions**, and a break in the main cable stops the whole network. It is cheap and uses little cable.

Mesh. Each device is linked to **at least one other**, usually several, so there are **multiple routes**. Devices **relay** packets on towards the destination by whichever route is available, so if one link fails, packets go another way. A mesh is **robust**, has few collisions and nodes can be added without disruption, but it needs many links and is expensive.



Hybrid. A mix, such as one star per floor with the switches joined by a mesh, combining the benefits of each part.

Choosing a topology: give a feature and why it matters there: a classroom suits a star (one faulty cable doesn't stop the lesson); links that must never fail suit a mesh.

Ethernet and CSMA/CD

Ethernet is the most common **protocol** (set of rules) for **wired LANs**. It sends data in **frames**, each with source and destination (MAC) addresses and error-checking data so damaged frames can be re-sent. It is not a cable.

When devices share one medium, two can start sending at once and their signals garble each other: a **collision**. Ethernet handles this with **CSMA/CD**. CSMA/CD itself does nothing; it is a set of rules, and each **device (workstation)** follows them:

1. **Carrier sense:** the device **listens** to the channel and only sends when it is **idle**.
2. **Multiple access:** all devices share the medium, so two can find it idle and start sending together.
3. **Collision detection:** a device that detects a collision **aborts** its transmission and sends a **jamming signal** so every device knows.
4. Each device waits a **random time** (back-off) before trying again, so they are unlikely to clash again.
5. After repeated collisions, the random wait time is **increased**.

In a star with a switch, each device has its own link, so collisions hardly happen.

Wired and wireless transmission

Medium	How it carries data	Strengths	Weaknesses
Copper cable	Electrical signals	Cheap, easy to install	Lower bandwidth, electrical interference, fades over distance, can be tapped

Medium	How it carries data	Strengths	Weaknesses
Fibre-optic cable	Pulses of light	Much higher bandwidth, little interference, long distances before a repeater, hard to tap	Costly, fragile
Radio waves (WiFi)	Electromagnetic waves, short range	No cables, devices can move	Walls and distance weaken it, interference, slower, less secure
Microwaves	Electromagnetic waves between dishes or masts	Long distances without cables	Need line of sight; weather
Satellites	Microwaves relayed by a satellite	Reach remote places and moving users	High latency, weather, costly equipment, line of sight

Wired is faster, more reliable, has less interference and is more secure (an attacker needs physical access), but devices are tied to one place and need cabling. **Wireless** gives mobility, no cabling, easy adding of devices (including visitors' own), but is less secure (signals reach anyone in range), slower, suffers interference and fades with distance. Many networks offer both.

LAN hardware and the router

- **Server:** provides a service (files, printing, web pages) to clients.
- **NIC:** connects a device to a wired network; has a unique **MAC address**.
- **WNIC:** the wireless version. Through its **antenna** it converts radio waves to digital data and back, **checks the address** of incoming data and ignores data for others, and **encrypts and decrypts**.
- **Switch:** the centre of a star. It **stores the MAC addresses** of connected devices, **receives packets** and **forwards each one only to its intended recipient**. (A **hub** sends every packet to every device.)
- **WAP:** lets **wireless devices connect to a wired network** by sending and receiving radio signals.
- **Bridge:** joins two LANs or segments that use the same protocol.
- **Repeater:** **regenerates (boosts) a weakened signal** so it can travel further.

A **router** joins **different networks**, such as a LAN and the internet. It **receives packets**, **reads the destination IP address**, and **forwards each packet towards its destination** using its **routing table**, which it **maintains** to find the most efficient route. It also **assigns private IP addresses** to LAN devices, **holds the LAN's public IP address**, and acts as a **gateway** (converting between protocols) and often a **firewall**. It does **not** find the IP address of a URL (the DNS does) or send packets to every device.

In a star LAN the router usually attaches to the **switch**, so every computer can reach it, or to the **server**, if the server checks all traffic.

Cloud computing

Cloud computing means using **storage, software or processing on remote servers**, reached over the internet, instead of your own hardware.

- A **public cloud** is run by a **third-party provider** for **anyone** who signs up. Customers share its hardware, but each customer's data stays private to them.
- A **private cloud** is **dedicated to one organisation**, reached over the internet or its own network.

Benefits: access **from anywhere** with internet; no servers to maintain; the provider does **backups and security**; capacity **grows quickly**; easy **sharing**. **Drawbacks:** **no internet, no access**; you **rely on the provider** for backups and security; **ongoing cost**; provider faults cut you off.

A **private** cloud gives the organisation **control over security, privacy and backups** and can be **tailored** to its needs. A public cloud suits a service everyone must reach, and sharing infrastructure is cheaper.

The internet and the World Wide Web

The **internet** is the global **network of networks**: the links, routers and protocols that carry data. The **WWW** is the **collection of web pages and resources** on web servers, reached with URLs and browsers, and runs **over** the internet. Webmail in a browser uses both.

Internet hardware:

- **Modem:** converts **digital data to analogue** for telephone lines, and back.
- **PSTN:** the telephone network, of many line types, so data may be converted to analogue; data flows both ways at once through **switching centres** and ISPs.
- **Dedicated (leased) line:** a **private, permanent** link for one organisation, with a fast, guaranteed rate.
- **Cell phone network:** land split into **cells**, each with a **mast and antenna** exchanging **low-power radio signals** with phones in the cell; many phones can use the same mast at once.

Bit streaming

Bit streaming is a **continuous, ordered flow of bits** over a communication path, so media plays **while it is still arriving**.

The data is **compressed** and sent from a **media server** into a **buffer** on the receiving device, which plays from it. The buffer covers differences between the arrival speed and the playing speed; if it runs empty, playback **pauses**.

- **Real-time (live):** sent **as it happens** (a live match, a video call); viewers can't skip ahead.
- **On-demand:** the file is **already stored** on the server and can be **paused, rewound and re-watched**.

Bit rate is the number of bits a stream needs per second; higher quality needs a higher bit rate, and the **broadband speed** must be at least that, or the buffer empties. A film streamed at 5 Mbps (1 Mbps = 10^6 bits per second) needs $5 \times 10^6 \div 8 = 625\,000$ bytes a second; a 2-hour film (7200 s) uses

$$\frac{5 \times 10^6 \times 7200}{8} = 4.5 \times 10^9 \text{ bytes} = 4.5 \text{ GB.}$$

On a 3 Mbps connection the buffer drains and the film keeps stopping. So video is **compressed** (usually **lossy**, which cuts far more data than lossless) and offered at lower bit rates, which means less bandwidth and less buffering.

IP addresses

Every device on the internet needs an **IP address**; routers use each packet's destination address to pass it on.

IPv4: 32 bits, as **four groups of 8 bits** in denary separated by **full stops**, such as 203 . 0 . 113 . 57. Each group is 0 to $2^8 - 1 = 255$. There are only $2^{32} = 4\,294\,967\,296$ (about 4.3 billion) addresses, too few for the world's devices.

IPv6: 128 bits, as **eight groups of 16 bits**, each written as **4 hexadecimal digits** (0000 to *FFFF*), separated by **colons**: $2^{128} \approx 3.4 \times 10^{38}$ addresses. **One run of consecutive groups that are all zeros can be replaced by a double colon ::**, only once per address. Leading zeros in a group may also be dropped.

2A02:0C7F:0000:0000:0000:0000:14B6:0009 → 2A02:0C7F::14B6:0009

Any other shape (a group above 255, a letter in a dotted address, the wrong number of groups, two ::) is **invalid**.

How a device gets its address: the **router** normally allocates one when the device joins the LAN, recording its MAC address; or it is set by hand.

- A **public IP address** is unique on the internet and **visible to any device on the internet**. The router has one so the LAN can be reached.
- A **private IP address** is used **only inside a LAN**, is **assigned by the router**, and can't be reached directly from the internet. Devices with only private addresses are **hidden behind the router** and its firewall, which is safer; a device with a public address can be attacked directly.
- A **static IP address** is **fixed**: it **does not change** when the device reconnects (servers need one so they can always be found).
- A **dynamic IP address** is **allocated each time** the device connects, so it **can change**.

These combine: an office printer might have a **static private** address, fixed and used only inside the LAN.

Subnetting

Subnetting divides one network into **smaller networks (subnets)**, for example one per department. An address then has two parts: the **network ID**, **the same for every device in the subnet**, and the **host ID**, which **identifies the device within its subnet**.

A **subnet mask** shows the split: its 255 groups (1 bits) cover the network ID and its 0 groups the host ID. For 172.16.40.9:

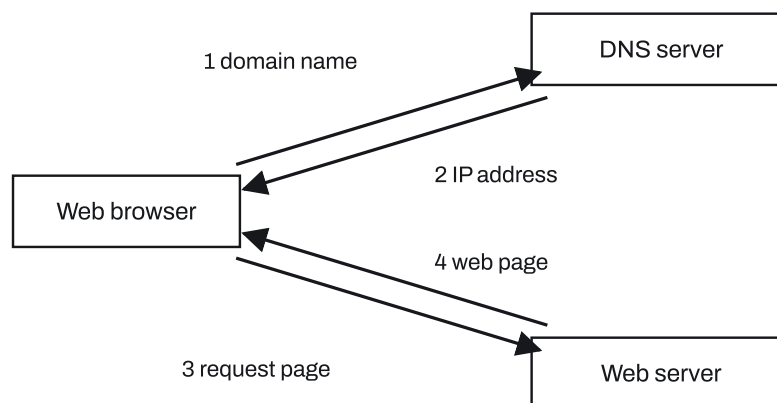
- with mask 255.255.255.0: network ID 172.16.40 (network 172.16.40.0), host ID 9;
- with mask 255.255.0.0: network ID 172.16, host ID 40.9.

Two devices are in the same subnet only if their network IDs match. Why subnet (reason **and** effect):

- **less traffic and congestion**: data between devices in one subnet stays there;
- **better security**: devices can be kept out of other subnets, so one compromised device can't expose the whole network;
- **easier management and maintenance**: faults are isolated, and one subnet can be changed while the rest keeps working;
- **easier growth**, one subnet at a time.

URLs and the DNS

A **URL** such as `https://www.example.org/timetable/week3.html` has a **protocol** (`https`), a **domain name** (`www.example.org`, the web server) and a **path** to the file. Routers need an IP address, not a name, so the **DNS** (Domain Name Service), a worldwide system of **DNS servers** holding tables of domain names and IP addresses, translates it. A DNS server that doesn't know a name asks another.



1. The browser **checks its cache** for the domain's IP address.
2. It **splits the URL** into its parts.
3. If needed, it **sends the domain name to a DNS server**, which **returns the matching IP address**; the browser caches it.
4. The browser **connects to the web server at that IP address** and **requests** the resource in the path.
5. The server sends the files back and the browser **renders** the page.

Key facts and formulas

There is no formula list in the 9618 exams, so every fact here is **Learn it**.

Formula	Status
IPv4: $4 \text{ groups} \times 8 \text{ bits} = 32 \text{ bits}$, denary, each group 0–255, full stops	Learn it

Formula	Status
IPv6: 8 groups $\times$ 16 bits = 128 bits, each group 4 hex digits (0000–FFFF), colons; one run of zero groups can become ::	Learn it
Number of addresses: IPv4 $2^{32} \approx 4.3 \times 10^9$; IPv6 $2^{128} \approx 3.4 \times 10^{38}$	Learn it
IP address in a subnet = network ID + host ID; mask bits 1 = network ID, 0 = host ID	Learn it
1 Mbps = 10^6 bits per second; 1 byte = 8 bits	Learn it
Data (bits) = bit rate (bits per second) $\times$ time (seconds)	Learn it
Time (seconds) = $\frac{\text{data in bits}}{\text{bit rate}}$	Learn it
Smooth streaming needs broadband speed $\geq$ the stream's bit rate	Learn it

How to do it

In the Paper 1 questions we have tagged for this topic (30 questions, 2021–2025, two of them repeated on a second paper), the types came up this often. 22 of the 30 questions mix types, so the counts add up to more than 30.

Question type	Questions
The router's role and functions	7
LAN and WAN characteristics and differences	7
Cloud computing	7
Transmission media, wired and wireless	7
Client-server, peer-to-peer, thin and thick clients	7
Types of IP address	7
CSMA/CD and Ethernet	6
IPv4 and IPv6 formats	5
Subnetting	5
Drawing a star topology	5
Other LAN hardware	5
Bus, star and mesh topologies	4

Question type	Questions
Packets between two hosts in a star	3
Bit streaming	3
Internet hardware	3
URLs, the DNS, the internet and the WWW	3

Almost every mark is **one per correct point**, tied to the situation. The facts are in "Understand it"; below is how to use them.

1. The router's role and functions (7 questions)

1. Use the router paragraph in "Understand it": one function per line, one more than the marks.
2. Apply each point to the scenario; "lets the devices connect to the internet" just repeats the question.

Variations: *tick whether the router does a task; which LAN device it attaches to*, with a real reason (see "Understand it"); *name device A* between a LAN and the internet: router.

2. LAN and WAN characteristics and differences (7 questions)

1. Characteristics: area, ownership of infrastructure, dedicated or not, data rate ("LAN and WAN" in "Understand it").
2. For **differences**, state both sides in one sentence: "A LAN covers a small geographical area, whereas a WAN covers a large one."

Variations: *benefits of a LAN*: sharing and central management, not "internet access"; *LAN or WAN? Justify*: one building is a LAN (small area, no leased media).

3. Cloud computing (7 questions)

1. **Define** it as services or storage on remote servers reached over the internet; don't define it with the word "cloud".
2. Choose benefits and drawbacks true of the **cloud specifically**: "needs an internet connection" is; "files can be lost" is true of any storage.
3. For a 2-mark "describe", give the point **and** its expansion: "Loss of control over backups, because the provider decides how the data is backed up."

Variations: *why a public cloud, or private instead of public* (last paragraph of "Cloud computing"); *name a cloud type and an application* ("public"; "email"), never brand names.

4. Transmission media, wired and wireless (7 questions)

1. Name the medium and what it carries: electrical signals, pulses of light, or electromagnetic waves.
2. Compare both sides: "fibre-optic has a higher bandwidth than copper".

3. Take advantages and drawbacks from the table, linked to the situation.

Variations: *why offer both; satellite vs copper; choose wired or wireless and justify:* usually no mark for the choice, so reasons tied to the use carry the marks (films and games: wired, for higher bandwidth and less latency).

5. Client-server, peer-to-peer, thin and thick clients (7 questions)

1. **Client-server roles:** name which device in the scenario is the server and which the client, then say what each does. Naming each device is often a mark on its own.
2. **P2P drawbacks** need point + expansion; "weak security" alone scores one mark at most.
3. **Thin vs thick:** who does the processing and where data is stored.

Variations: *"why is this client-server?":* map the scenario onto the roles (data on a web server; each browser a client sending requests); *thin-client table:* a characteristic plus its use in the scenario.

6. Types of IP address (7 questions)

1. Learn the four one-sentence definitions (public, private, static, dynamic) and join two for a combined term such as **static private**.
2. In matching tasks, ignore descriptions that sound plausible but aren't the definition, such as "goes up by 1 each time the device connects".

Variation: *why the router has both:* public so the LAN is visible to and reachable from the internet; private so the router is identified by the computers inside the LAN.

7. CSMA/CD and Ethernet (6 questions)

1. Write the five steps from "Understand it" in order, with the **device** as subject of each: "the device listens", never "the protocol listens".
2. **"A collision is detected; describe how it is managed":** only the steps from the collision on.

Variations: *drawbacks of CSMA/CD:* waits can grow without limit; no device can be given priority; short distances only; more devices mean far more collisions. *Describe Ethernet:* protocol for wired LANs, uses CSMA/CD, frames with addresses and error checks.

8. IPv4 and IPv6 formats (5 questions)

1. **Differences:** compare, for example "IPv4 has 4 groups; IPv6 has 8", "32 bits vs 128 bits", "denary vs hexadecimal". The separator only counts if the question hasn't given it.
2. **Why a dotted address is not IPv6:** it has only four groups, not eight; it uses full stops, not colons; it is 32 bits, not 128.
3. **Classify and justify:** usually no mark for the choice, so rule out **both** formats: 81 . 300 . 2 . 7 is not IPv4 (300 > 255) and not IPv6 (full stops, four groups), so invalid.

9. Subnetting (5 questions)

1. **Benefits:** each with its reason, from "Subnetting" in "Understand it". Benefits of networks in general (file sharing) don't count.
2. **The two parts:** name them **network ID** and **host ID**, then say which is shared and which is unique.
3. **With a mask:** 255 groups give the network ID, 0 groups the host ID: 10 . 40 . 7 . 25 with 255 . 255 . 255 . 0 has network ID 10 . 40 . 7, host ID 25.

10. Drawing a star topology (5 questions)

1. Draw the central device (a switch, or a router or server if the question says so).
2. Join **every** other device **directly** to it, and draw **no other lines**.
3. **Label every device** with the question's words.
4. If a router or modem gives internet access, connect it to the switch (or server) too.

11. Other LAN hardware (5 questions)

1. Give each device's **purpose** from the list in "Understand it", not what it looks like.
2. In "complete the table", work backwards from the description: "restores the signal over a greater distance" is a repeater.

Variation: *devices to connect a room of computers:* switch, hub or router.

12. Bus, star and mesh topologies (4 questions)

1. **Tick tables:** star = one central device; bus = shared central cable, most collisions; mesh = multiple paths, survives a failed line.
2. **Advantages over a bus:** point + expansion in context, such as "fewer collisions, because each computer only shares its link with the switch, so lessons aren't slowed".
3. **Identify and justify:** devices each linked only to the router form a star; justify with something new, such as each device's data not being sent to the others.

13. Packets between two hosts in a star (3 questions)

Give the three steps in "Topologies": to the central device (switch, or router if that is the centre); it reads the destination address; it forwards only to that device.

14. Bit streaming (3 questions)

1. **Explain real-time streaming:** the steps in "Bit streaming" in order (compressed, continuous bits, media server, buffer, why the buffer, play from it).
2. **Real-time vs on-demand:** live vs stored; can't vs can pause and re-watch.

Variations: *why compress first* (less bandwidth and buffering, so no one falls behind); *lossy or lossless*: lossy, as it cuts far more data; *calculations*: $\text{data} = \text{bit rate} \times \text{time}, \div 8$ for bytes.

15. Internet hardware (3 questions)

State what each does in the network, using the four bullets in "Understand it"; for the cell phone network give the cells, the mast and antenna, and the low-power radio link.

16. URLs, the DNS, the internet and the WWW (3 questions)

1. **URL to web page** (4 marks): the five steps in "URLs and the DNS", one point each.
2. **Internet or WWW or both?** Say which **and** why: the internet carries the data; the WWW is used when a website is.

Worked examples

The bold codes show where marks are earned, as in Cambridge mark schemes. The number is how many marks.

- **M1** method mark: for a correct method, even if the numbers slip.
- **A1** accuracy mark: for a correct answer; it needs the M mark before it.
- **B1** mark for a correct result on its own, with no method needed.

Example 1

A dental clinic has a LAN with four computers, a server, a printer, a switch and a router that connects to the internet.

(a) Draw the network as a star topology. Label all devices. **[3]**

(b) A receptionist prints a letter from Computer 2. Explain how the data is transmitted to the printer. **[3]**

(a) A switch in the centre, with the server, printer, router and all four computers each joined to it by their own line, and no other lines: **B1** for the computers and server joined only to the switch, **B1** for the printer and router joined to the switch, **B1** for every device labelled.

(b) Computer 2 sends the packets to the switch **B1**. The switch reads each packet's destination address and looks it up in its table of connected devices **B1**. It forwards the packets only to the printer, not to the other computers **B1**.

Example 2

A company's LAN is divided into subnets. A laptop in the finance office has IP address 10 . 24 . 6 . 130 and subnet mask 255 . 255 . 255 . 0.

- (a) Identify the network ID and the host ID of the laptop. **[2]**
- (b) A printer in the design office has IP address 10 . 24 . 9 . 5 with the same subnet mask. State whether the printer and the laptop are in the same subnet. Justify your answer. **[2]**
- (c) Describe **two** reasons why the company uses subnetting. **[4]**
- (d) The company's web server has the IPv6 address 2001 : 0DB8 : 0000 : 0000 : 0000 : 0000 : 0A1F. Write this address in its shortest form using a double colon, keeping leading zeros. **[1]**

(a) The mask's three 255 groups cover the network ID. Network ID 10 . 24 . 6 **B1**; host ID 130 **B1**.

(b) Not in the same subnet **B1**: the printer's network ID is 10 . 24 . 9, which is different from the laptop's 10 . 24 . 6 **B1**.

(c) Two reasons, each with its expansion:

- To reduce traffic **B1**: data sent between devices in the finance subnet stays in that subnet, so the rest of the network isn't congested **B1**.
- To improve security **B1**: devices in other offices can't reach the finance subnet, so a compromised device can't expose the finance data **B1**.

(d) Groups 3 to 7 are a run of five zero groups, which becomes ::. So 2001 : 0DB8 :: 0A1F **B1**.

Example 3

A sports club streams its matches live on its website. The stream has a bit rate of 4 Mbps.

- (a) Explain how real-time bit streaming delivers the match to a viewer. **[4]**
- (b) Calculate how much data, in gigabytes, a viewer receives during a 90-minute match. Show your working. **[2]**
- (c) A viewer's broadband speed is 2.5 Mbps. Explain the effect on the viewer, and suggest how the club could help. **[3]**

(a) Any four: the video is compressed **B1**; it is transmitted continuously as a series of bits **B1** to a media server, which sends it on to viewers **B1**; the data arrives in a buffer on the viewer's device **B1**; the buffer holds data until the device can play it, covering differences between the speed of transmission and of playback; the viewer watches from the buffer.

(b) 90 minutes = 5400 seconds. Data = $\frac{4 \times 10^6 \times 5400}{8} = 2.7 \times 10^9$ bytes **M1** = 2.7 GB **A1**.

(c) The viewer receives only 2.5 of the 4 megabits needed each second **B1**, so the buffer empties and the video keeps pausing to buffer (and falls further behind the live match) **B1**. The club could offer a lower-quality stream with a lower bit rate, for example 2 Mbps, which the connection can keep up with **B1**.

Example 4

A photography club has six computers connected by a bus network using Ethernet.

(a) Describe how the computers use CSMA/CD to deal with collisions. **[4]**

(b) The club is choosing between a peer-to-peer model and a client-server model for sharing members' photos. Describe **two** drawbacks to the club of a peer-to-peer model. **[4]**

(a) Any four:

- A computer listens to the shared cable before sending, and only sends when it is idle **B1**.
- Because all six computers share the same cable, two can start sending at the same time, causing a collision **B1**.
- When a computer detects the collision, it stops transmitting and sends a jamming signal **B1**.
- Each computer waits a random time before trying again **B1**; after repeated collisions, the wait gets longer.

(b) Two drawbacks, each with its expansion:

- There is no central backup **B1**, so if a member's computer fails and they haven't backed up their photos, the whole club loses them **B1**.
- Photos may not be available **B1**, because a photo stored on a member's computer can't be reached while that computer is switched off **B1**.

Common mistakes

- **Vague comparisons.** "A LAN is faster" or "a LAN is local and a WAN is wide" repeat the name. Say "the data transfer rate of a LAN is higher than that of a WAN" and "a LAN covers a small geographical area".
- **Saying the protocol does things.** CSMA/CD is a set of rules; the **devices** listen, send the jamming signal and wait.
- **One-word drawbacks.** "Weak security" doesn't describe anything. Add why: "no central security, so the network is only as secure as its weakest computer".
- **Cloud answers that fit any storage.** "The data can be lost" or "it is secure" apply to a hard disk too. Say something only true of the cloud: needs the internet, relies on the provider for backups, recurring cost.
- **Public cloud = public data.** A public cloud is a service anyone can sign up to; your files in it are still private to you. A private cloud is private to an **organisation**, not to one person.
- **Network IP and host IP.** The parts of the address are the **network ID** and the **host ID**.
- **A single colon for zero groups.** Consecutive zero groups in IPv6 are replaced by a **double colon**, and only once.

- **Describing instead of explaining a buffer.** Say **why** it is used (to cover differences in speed between arrival and playback), not only what it stores.

How to get the marks

- **One mark, one point.** Mark schemes list separate points; write each on its own line, and give one more than the marks if you can.
- **"Describe"** means say what it is or what happens, with detail; a bare word ("security") rarely scores. **"Explain"** means give reasons: add "because..." or "so that...". **"Identify"**, **"State"** and **"Give"** need a short, precise answer. **"Justify"** means reasons for your choice, often with no mark for the choice itself.
- **Point + expansion.** Questions worth 2 marks per item (drawbacks of P2P, reasons for subnetting, star vs bus) give one mark for the point and one for developing it. Use "...because..." or "...so...".
- **Use the context.** Name the scenario's devices and users; generic lists lose marks where the question asks "to the students" or "in this network".
- **Compare both sides** in "difference" questions, in one sentence.
- **Tick tables:** one tick per row unless told "one or more". **Diagrams:** every device labelled, nothing extra.
- **Calculations** (bit streaming): show the working ($\text{bits} \times \text{seconds} \div 8$), and give units.

Quick check

1. State **three** differences between an IPv4 address and an IPv6 address.
2. For each address, state whether it is a valid IPv4 address, a valid IPv6 address or invalid, and give a reason: (a) 172.16.300.4 (b) FD00::7:2B (c) 81.2.69.160 (d) 2001:DB8::1::5.
3. A 1.2 GB video is downloaded over a 40 Mbps connection. Calculate how long the download takes, in minutes. (Take 1 GB = 10^9 bytes.)
4. A device has the IP address 192.168.50.77 and subnet mask 255.255.0.0. Identify its network ID and host ID.

Answers

1. Any three: IPv4 is 32 bits, IPv6 is 128 bits; IPv4 has 4 groups, IPv6 has 8; IPv4 groups are denary (0–255), IPv6 groups are hexadecimal (0–FFFF); IPv4 uses full stops, IPv6 uses colons; IPv6 can use :: for a run of zero groups.
2. (a) Invalid: it has full stops like IPv4, but $300 > 255$, and it isn't IPv6 (no colons). (b) Valid IPv6: hexadecimal groups separated by colons, with one :: standing for five zero groups. (c) Valid IPv4: four denary groups, each from 0 to 255, separated by full stops. (d) Invalid: :: appears twice, so you can't tell how many zero groups each one replaces.
3. $1.2 \times 10^9 \times 8 = 9.6 \times 10^9$ bits. Time = $\frac{9.6 \times 10^9}{40 \times 10^6} = 240$ seconds = 4 minutes.
4. The mask has two 255 groups, so the network ID is 192 . 168 and the host ID is 50 . 77.

Past questions to try

- **9618/13/M/J/21 Q4**: peer-to-peer drawbacks, what a router does, wired or wireless, internet vs WWW.
- **9618/12/M/J/22 Q9**: network devices, fibre-optic vs copper, CSMA/CD.
- **9618/13/O/N/22 Q7**: a cloud diagram, satellites vs copper, and reading IDs with a subnet mask.
- **9618/11/M/J/25 Q2**: real-time bit streaming, compression, modems and dedicated lines.