Questions matter

Teaching guide: Fundamentals of computer networks

This resource supports Section 3.5 of the GCSE Computer Science specification (8525), mostly centred around Paper 2.

Version 1.0
September 2025

Contents

Computer networks

A computer network is two or more computers or devices linked together to communicate and share resources.

These connections can be:

- wired: using copper or fibre-optic cables (a physical connection)
- wireless: using technologies such as Bluetooth or Wi-Fi.

Why are networks useful?

Computer networks allow users to:

- **share resources**: files, printers and internet connections can be accessed by multiple users
- **collaborate**: users can work together in real time using tools like shared documents, video conferencing and messaging apps
- **access services**: stream media (TV, music), play online games, use cloud applications and storage
- **increase efficiency**: share data, avoid duplication of files and update software across multiple devices at once
- **manage security**: centralise user login and authentication, apply access controls, install firewalls and antivirus software, and monitor activity to protect data.

Devices that can be part of a network may include:

- computers
- smartphones and tablets
- car infotainment systems
- printers
- servers.

These devices communicate with each other using **established protocols**.

A **network protocol** is defined as a set of rules and standards that govern how data is transmitted and received over a computer network. For example:

- the Hypertext Transfer protocol (HTTP) is used for accessing websites
- SMTP is used for accessing email
- Wi-Fi is a set of standards based on the IEEE 802.11 protocols (Knowledge of Wi-Fi is not required for the AQA GCSE 8525 specification).

Students should be able to:

- define the term network protocol
- explain the purpose of common network protocols.

Common network protocols

Students should know what each protocol is used for. For the GCSE exam, the first bullet point in the following table is sufficient – subsequent bullet points provide more technical detail which may help students to understand the purpose of common network protocols.

Protocol	What the protocol is used for
TCP (Transmission Control Protocol)	• Whenever reliable communication over a network is needed, e.g. browsing websites, sending emails, downloading files. • Splits data into packets and ensures they are delivered correctly and in the right order.
IP (Internet Protocol)	• Handles packet routing and addressing across networks. • Adds source and destination IP addresses to data packets so they can be routed to the correct destination.
HTTP (Hypertext Transfer Protocol)	• Accesses and loads web pages: HTTP is used to retrieve content from web servers so a browser can display web pages to users. • Data transmission is not secure. • A client sends an HTTP request, the server responds with the requested data (e.g. HTML, references to resources like images and style sheets/CSS files). • Transfers data to the server, e.g. when submitting online forms.
HTTPS (Hypertext Transfer Protocol Secure)	• Provides an encrypted version of HTTP for more secure web browsing and transactions. • Uses encryption protocols such as SSL/TLS to protect data.
SMTP (Simple Mail Transfer Protocol)	• Sends outgoing emails from a client (like Outlook, Mail or Gmail) to a mail server. • Transfers emails between mail servers. • SMTP is only used for sending emails not for receiving or retrieving them.
IMAP (Internet Message Access Protocol)	• Retrieves incoming emails from a mail server. • Emails are stored on the server, not permanently downloaded to one device. • Allows users to view or organise emails on multiple client programs or devices. • Emails are synced across devices. For example, if you delete an email on your laptop, it will also be deleted from your phone.

Types of computer network

There are three main types of computer network:

1. **Personal Area Network (PAN)**
    - Very short range (typically under 10 metres).
    - Connects personal devices like phones, smartwatches, wireless keyboards.
    - Example: Bluetooth earbuds connected to a smartphone.

2. **Local Area Network (LAN)**
    - Covers a small area like a home, school or office.
    - Devices are connected by Ethernet or Wi-Fi.
    - Example: home network linking computers, printers and smart TVs.

3. **Wide Area Network (WAN)**
    - Covers large geographical areas (e.g. cities, countries).
    - Connects multiple LANs via telephone lines, fibre optics or satellites.
    - Example: The internet is the largest WAN.

1. Personal Area Network (PAN)

A PAN (or WPAN – Wireless Personal Area Network) is the smallest type of computer network, used for **short-range communication**, typically within 10 metres.

How PANs connect devices:

- **wired connections**: for example, USB cables
- **wireless technologies**: most commonly Bluetooth or Wi-Fi Direct.

For the GCSE exam, only Bluetooth wireless technologies need to be considered. For context, it may be useful to know that Bluetooth PANs have largely replaced infrared PANs which:

- were typically two devices, e.g. the remote control and a television
- needed a clear line of sight between the remote control and the receiver.

As with infrared, PANs are designed to connect personal devices in your immediate area – often without needing an internet connection.

There are relatively few resources on PANs, which this resource attempts to counter, though many students will use PAN devices every day without realising, for example, AirPods use a Bluetooth PAN.

Examples of PAN devices and uses

- **Bluetooth remote controls**: Devices like Sky Q or Apple TV remotes use Bluetooth instead of infrared. No line-of-sight needed and connect instantly to the device.
- **File sharing** (e.g. AirDrop, Wi-Fi Direct):
    - Apple's AirDrop uses Bluetooth to establish a PAN connection then switches to Wi-Fi to transfer files quickly between nearby Apple devices.
    - Wi-Fi Direct used by many Android and Windows devices to share files in a similar way.

- **Peer-to-peer payments**: Banking apps, like Monzo, use Bluetooth to allow users nearby to send money without needing to enter account details.
- **Wearable health and fitness technology:** PANs connect smartwatches, fitness bands or medical monitors to a smartphone's health app for real-time tracking and updates.

Key characteristics of a PAN	Typical uses of PAN
Short range communication – typically less than 10 metres	Where low power use and minimal interference is important, e.g.: • Bluetooth mice and keyboards • wearable technology • portable bank card readers, e.g. SumUp.
Connects personal devices	Links phones/tablets, wearables, games controllers and headphones.
Limited number of devices	Bluetooth PANs typically support up to eight active devices.
Wired or wireless (WPAN)	• Wired USB connections between devices. • Wireless streaming of music to Bluetooth earbuds or speakers.
Portable, does not (usually) require Wi-Fi or an internet connection	Designed to move with the user, e.g.: • earbuds • health and fitness monitoring • file transfer between nearby devices.
Low power consumption	PANs prioritise battery life over speed, e.g.: • rechargeable devices • smart home devices such as doorbells, lightbulbs and sensors.
Lower bandwidth than a LAN	• A keyboard sends keystrokes. • A smartwatch sends steps or heart rate every few seconds. • A Bluetooth headset streams compressed audio (to a limited number of users).
Can be secured through encryption, passkeys or pairing to protect sensitive data	• Health monitoring. • Assistive technology such as hearing aids. • In-vehicle technology, e.g. hands-free calling, infotainment systems, keyless start, diagnostics. • Authentication and access control. • Peer-to-peer payments (e.g. nearby friends in a banking app).

Advantages of a PAN	Explanation
Supports a wide range of personal devices	Works with phones, wearables, earbuds, etc.
Enables user mobility	Stay connected while moving, e.g. Bluetooth earbuds with phone in pocket.
Lower bandwidth	There is no need for high bandwidth with multiple streams like video streaming or large file downloads.
Low power consumption	Ideal for battery-powered devices like fitness trackers and smartwatches.
Inexpensive and requires minimal additional equipment	No need for routers or access points.
Easy to set up and use	Devices can quickly pair and sync via Bluetooth or USB.
Flexible device management	Devices can be easily added or removed.
Secure communication possible	Encryption, pairing, and authentication can protect data.
Reduces cable clutter	Enables wireless connections between devices.

Disadvantages of a PAN	Explanation
Limited range	A PAN connection is only stable within about 10 metres. For example, if you're streaming music from your phone to Bluetooth earbuds, the connection may start to break up if you move too far away – such as leaving your phone in one room while walking around the house. This limitation is due to the short-range nature of technologies like Bluetooth, which prioritise low power use over long-distance coverage.
Lower speed	Bluetooth is often slower than Wi-Fi or wired alternatives.
Not ideal for large files	Transferring large files over Bluetooth can be slow and unreliable.
Limited number of devices	Only a few devices can connect at the same time (e.g. 7–8 in Bluetooth).

Disadvantages of a PAN	Explanation
Risk of interference	Can suffer from signal disruption due to other wireless devices.
Security risks	Susceptible to hacking if not properly secured (e.g. weak pairing).
Battery drain	Frequent Bluetooth use can reduce battery life on mobile devices.

2. Local Area Network (LAN)

A Local Area Network is computer network that covers a **small geographical area** such as a home, school or office.

LANs are usually owned and managed by a single person or organisation.

How LANs work

- In most homes, wireless devices connect to a router via Wi-Fi forming a LAN.
- In schools and businesses, LANs often use a mix of wired and wireless connections.
- It's possible to have multiple LANs within one building or campus.

3. Wide Area Network (WAN)

The Internet is the biggest example of a WAN.

- A WAN covers a **wide geographic area**, often connecting cities, countries or even continents.
- Multiple networks are connected together – for example, a business may link offices in different countries.
- Usually under collective or distributed ownership – no single organisation owns the whole WAN (e.g. the Internet is shared by many companies and users).

Network cables

Students should know that wired networks can use different types of cable, such as fibre and copper, and when each would be appropriate.

Copper cables (Ethernet/twisted pair)

- Transmit data using electrical signals.
- Are commonly used inside homes, schools and offices, for short to medium distances.
- Are slower than fibre.
- Are less reliable, especially if the cable is old or corroded (some are at least 60 years old).

Broadband connections often use the old telephone network (PSTN), which was built with copper wiring. These are gradually being phased out and replaced with fibre optic networks.

Fibre optic cables

- Use light signals to transmit data through glass or plastic fibres.
- Are used for reliable high-speed broadband in homes and schools.
- Support much faster data transfer speeds than copper.
- Support long-distance connections (e.g. between countries, cities or from the service provider to a home or school).

Types of fibre broadband:

- Fibre to the Cabinet (FTTC) runs a fibre optic cable from the telephone exchange to a street cabinet then a copper cable from the cabinet to your home. The copper cable slows the connection down: it is not capable of transmitting data as fast as fibre optic cable and may be worn and corroded.
- Fibre to the Home (FTTH) runs a fibre optic cable directly from the service provider's exchange into your home, school or office. No copper cable is used. This means that the connection is much faster and more reliable.

Advantages of fibre optic cables:

- much faster data transfer speeds
- greater stability and reliability compared to copper
- less interference than copper
- better for streaming, gaming
- more future proofed – copper networks are gradually being replaced by fibre optic networks.

Wireless and wired networks

Students should be able to discuss the advantages and disadvantages of wireless networks as opposed to wired networks.

Advantages of a wireless network	Explanation
Mobility portability	• Users can move around freely while staying connected. • Devices like laptops, tablets and smartphones don't need cables.
Ease of access	• Devices can connect to networks quickly and easily with no wiring. • Easy to set up in different locations.
Less installation time/cost	• No need to run long cables through walls or ceilings. • Routers generally accept more wireless connections than physical connections.
Device compatibility	Most modern devices have built-in Wi-Fi capability.
Supports BYOD (Bring Your Own Device)	Allows people to bring in their own devices to school, college and the office.
Remote access	Enables access to files, systems and emails from anywhere with Wi-Fi.
File sharing and communication	Users can join video calls or easily share resources such as files and printers.
Scalability	Easy to expand the network by adding more wireless devices without adding cables or more hardware.

Advantages of a wired network	Explanation
Speed	• Typically, much higher data transfer rates than wireless networks.
Stability/less interference	• Provides a more stable connection with fewer dropouts – ideal for gaming, streaming or transferring large files. • Less prone to interference from other devices, walls or signals compared to wireless.
Higher bandwidth	• Less competition for bandwidth as each device has its own direct (Ethernet) connection. • Cables can handle large amounts of data with very little interference compared to wireless (e.g. they are not limited by frequency).
Security	More secure than wireless networks – data travels through cables and is harder to intercept than a wireless signal.
Low latency	Lower delay in data transmission compared to wireless – important for real-time applications like multi-player online gaming.
Automatic connection	Devices connect automatically to the LAN when the cable is connected (usually no need to enter passwords or network settings).
Long-term reliability	Once installed, a wired network tends to last longer, need fewer upgrades and require less maintenance over time.

Disadvantages of a wireless network	Disadvantages of a wired network
More susceptible to interference – signal/connection may be affected by walls, windows, devices, appliances or other networks.	Limited device compatibility, e.g. devices need an Ethernet port or adapter.
Limited range – signal gets weaker as you move away from the wireless access point.	Difficult/time consuming to install and expand.
Lower data transfer speeds, especially when multiple devices are connected at once.	Lack of mobility/portability – devices must stay physically connected.
Wireless connections drop more frequently.	Requires extra hardware (so installation costs can be higher), e.g. cables, couplers/connectors, network cards, switches, wall sockets etc.
Easier to hack/less secure – wireless signals can be intercepted unless strong encryption is used (e.g. WPA3).	
Lower bandwidth – lower bandwidth shared with all devices on the same wireless channel which can slow down performance.	
Higher latency.	
Devices operate on different frequencies, e.g. 2.4GHz-only devices cannot connect to a 5GHz-only network.	

Network security

Students must understand the need for, and importance of, network security. Network security is essential in protecting data, systems and people from threats and misuse.

This is a key topic which appears in several areas of the specification in relation to Paper 2, namely:

- 3.5 Fundamentals of computer networks
- 3.6 Cyber security
- 3.8 Ethical, legal and environmental impacts of digital technology on wider society, including issues of privacy

This broadly falls into three areas:

- the cyber security measures producers use to protect their networks, websites and data
- the measures users can take to protect themselves and their network from attack
- the ethical and legal challenges of implementing these measures, particularly in relation to young people, e.g. the individual vs the State; the right to freely access the Internet vs the Online Safety Act.

Discussion of some of the examples of PAN devices, such as wearable technologies, may help students prepare to explain the 'impacts and risks of digital technology on society' in Section 3.8 of the specification.

Impacts and risks of networks on society

Data privacy risks

- Personal data can be intercepted by hackers if connections are insecure.
- Devices often share sensitive data like location, health statistics or voice commands.
- Companies managing these devices might misuse or sell personal data.

Security challenges

- Bluetooth and other technology can be vulnerable if not properly secured.
- Wearable devices can be hacked to track users or access other linked devices.

Measures

- Use devices with the latest Bluetooth technology which is more secure.
- Protect devices with strong passwords.
- Make sure encryption and security features are enabled.
- Be careful when using public or untrusted networks.
- Remove devices that you don't recognise.
- Keep software and firmware updated.
- Research and understand how personal data is used, for example by looking at the terms and conditions when signing up.
- Limit data sharing and permissions.

Importance of network security

The importance of network security is usually best communicated in terms of devices and programs that the students use every day, for example email on their phone, and can be tied to the school's policies on personal safety and network security. Cyber security (the processes, practices and technologies designed to protect networks, computers, programs and data from attack, damage or unauthorised access) is likely to be everything the school is already doing and with which the student is familiar. For example, the measures that a student can take to protect themselves (from phishing, shouldering) and methods that web producers use to protect their websites (email confirmations, CAPTCHA).

Students should be able to explain the following methods of network security:

Security method	Explanation

Authentication
Examples:
• Entering a username and password.
• Using two-factor authentication (2FA) (e.g. a code sent to your phone or email).
• Using biometrics such as fingerprint or facial recognition.
	• Authentication is the process used to verify the identity of a user or device before granting access to a system or network.
	• Authentication aims to prevent unauthorised access and ensure that only authorised users can access the network or sensitive data.
	• **Links to programming skills:**
	  ○ Paper 1
	  ○ *3.2.11 Be able to write simple authentication routines.*

Encryption Examples: • HTTPS encrypts data sent from your browser to the web server. • Messaging apps like WhatsApp use • end-to-end encryption: "No one outside of the chat, not even WhatsApp, can read, listen to, or share them. This is because with end-to-end encryption, your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them." [1]	• Encryption scrambles data/changes plaintext into ciphertext (before transmission) so that it cannot be read without a decryption key. • Encryption aims to protect data from unauthorised access.
Firewall A firewall attempts to block unauthorised access to or from a private network, such as hackers or malware trying to get in.	A firewall is a network security device (or software) that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

[1] https://faq.whatsapp.com/820124435853543

Security method	Explanation
MAC address filtering • A MAC (Media Access Control) address is a **unique identifier** assigned to a device's network adapter. • A physical address embedded within the device's network adapter, used to identify a device on a network. • 6 pairs of hexadecimal characters (0–9, A–F), separated by a colon, e.g. A0:B1:C2:D3:E4:F5 • An iPhone has at least two MAC addresses: one for the Wi-Fi interface and another for Bluetooth. • These can be viewed in Settings > General > About	• MAC address filtering is a network security method that allows devices to access or be blocked from accessing a network based on their MAC address. • For example, a router usually has a MAC address printed on the back. This MAC address could be used to block the router from accessing certain web resources. • Some privacy features, such as on an iPhone, use a new virtual (private) MAC address each time a connection is made. These override the embedded MAC address to prevent tracking or MAC address filtering based on your device's MAC address.

How security methods work together

Students should understand how these methods can work together to provide a greater level of security, e.g.:

What happens when a laptop connects to a public Wi-Fi hotspot?

MAC address filtering

- When a user tries to connect to a public Wi-Fi hotspot, the router first checks the device's MAC address.
- If the MAC address is on a deny list (e.g. the user was previously banned for violating terms), access is denied.
- If the MAC address is not blocked, the device is allowed to connect to the network.

Firewall protection

- Once connected, a firewall monitors and filters incoming and outgoing traffic.
- It may block:
  - common attack methods such as unsafe ports or protocols
  - malware activity such as attempts to contact suspicious servers
  - non-essential services like streaming, to conserve bandwidth (especially on networks when capacity is limited, e.g. trains)
  - access to banned or illegal websites.

Limitations of the firewall

- If the user uses a VPN, or the data is encrypted (e.g. via HTTPS), the firewall may not be able to inspect the contents of the packets.
- This can limit the firewall's ability to filter or block specific content or services.

Summary

- Authentication protects access to the system.
- Encryption protects data while it's being transmitted.
- Firewall protects the gateway between a network and the outside world.
- MAC filtering controls which devices can connect, e.g. by using an allow list.

TCP/IP model

Students should be able to name the four layers of the TCP/IP model and describe their main function(s) in a networking environment. The first bullet in each row covers the specification content required for the exam. Subsequent bullets provide more detail, for example how the link layer and Bluetooth are related.

Layer	Protocols	Main function
Application	HTTP HTTPS SMTP IMAP	• Where the network applications, such as web browsers or email programs, operate (i.e. where apps access the network). • Provides services and user interface for applications like web browsers and email clients.
Transport	TCP	• Sets up the communication between the two hosts (source and destination) and they agree settings such as the size of packets. • Splits data into packets and ensures reliable delivery in the correct order.
Internet	IP	• Addresses and packages data for transmission. Routes the packets across the network. • Adds source and destination IP addresses to packets. Handles routing of packets across different networks (e.g. through routers).
Link	Ethernet WPA2 WPA3 (Note: these link protocols are not in this specification)	• Where the network hardware such as the NIC (network interface card/adapter) is located. OS device drivers also operate here. • Deals with the physical connection to the network. • Device drivers control how data is sent and received via specific hardware (e.g. Ethernet, Bluetooth).