NETWORKS

OCR GCSE Computer Science

Network Types • Hardware • Topologies • Protocols

The Internet • OSI & TCP/IP Models • Network Security

Contents

1 What is a Network? 3
- 1.1 Why Do We Use Networks? . . . 3
- 1.2 LAN and WAN . . . 3
- 1.3 Other Network Types . . . 3

2 Network Hardware 4
- 2.1 Hubs vs Switches . . . 4
- 2.2 The Role of a Router . . . 4

3 Network Topologies 5
- 3.1 Star Topology — The Industry Standard . . . 5
- 3.2 Bus Topology — Simple but Flawed . . . 6
- 3.3 Ring Topology . . . 6
- 3.4 Mesh Topology — Most Reliable . . . 6

4 Wired vs Wireless Networks 6
- 4.1 Types of Transmission Media . . . 6

5 The Internet 7
- 5.1 IP Addresses . . . 7
- 5.2 Public vs Private IP Addresses . . . 7
- 5.3 DNS — The Internet's Phone Book . . . 7
- 5.4 Hosting and Cloud Computing . . . 8

6 Network Protocols 8
- 6.1 Common Protocols . . . 9
- 6.2 TCP and UDP . . . 9

7 The OSI and TCP/IP Models 10
- 7.1 The OSI Model (7 Layers) . . . 10
- 7.2 The TCP/IP Model (4 Layers) . . . 10

8 Network Security 11
- 8.1 Common Threats . . . 11
  - 8.1.1 Malware . . . 11
  - 8.1.2 Phishing . . . 11
  - 8.1.3 Denial of Service (DoS) and DDoS . . . 11
  - 8.1.4 Man-in-the-Middle (MitM) . . . 11
  - 8.1.5 SQL Injection . . . 11
- 8.2 Security Measures . . . 12
  - 8.2.1 Firewalls . . . 12
  - 8.2.2 Encryption . . . 12
  - 8.2.3 Authentication and Access Control . . . 12
  - 8.2.4 MAC Address Filtering . . . 12

9 Client-Server and Peer-to-Peer Networks 12
- 9.1 Client-Server Architecture . . . 12
- 9.2 Peer-to-Peer (P2P) Architecture . . . 13

10 Bandwidth, Latency and Packet Switching 13

10.1 Bandwidth and Latency 13
10.2 Packet Switching 14

11 VLANs and Cloud Computing **14**
11.1 VLANs 14
11.2 Cloud Computing 14

12 Key Terms Glossary **17**

1 What is a Network?

A **computer network** is a collection of two or more computing devices connected together so they can share data, resources, and services. Rather than each computer having its own isolated copy of everything, a network allows devices to communicate — sending files, accessing the internet, using shared printers, and much more.

1.1 Why Do We Use Networks?

Networks exist because sharing is more efficient than duplicating. Imagine a school where every computer had its own printer, its own internet connection, and its own copy of every piece of software — the cost would be enormous. Instead, a network allows all those resources to be centralised and shared. Networks also enable real-time communication and collaboration: two people on opposite sides of the world can edit the same document simultaneously, video call each other, or send messages in an instant.

1.2 LAN and WAN

Networks are categorised by their **geographical size**. The two most important types for GCSE are the **LAN** and the **WAN**.

LAN — Local Area Network	WAN — Wide Area Network
Covers a **small geographical area** — typically a single building or site, such as a school, home, or office.	Spans a **large geographical area** — cities, countries, or the entire planet.
The networking hardware is **owned and managed by the organisation** itself.	WAN infrastructure is typically **owned by telecoms companies** (e.g. BT) and leased to the organisation.
LANs are fast because distances are short and infrastructure is dedicated. A school LAN lets students log in anywhere and access files from a central server.	The **internet** is the world's largest WAN. A company with offices in London and New York uses a WAN to connect them, via leased lines, fibre-optic cables, or satellites.

LAN vs WAN — Key Points

Coverage: LAN = one site. WAN = multiple sites across large distances.
Ownership: LAN owned by the organisation; WAN leased from a third party.
Speed: LANs generally faster due to shorter cable runs and dedicated equipment.
Security: WANs carry more risk because data travels through networks you don't control.

1.3 Other Network Types

A **PAN (Personal Area Network)** is the smallest type — it connects personal devices like a phone and a smartwatch, often via Bluetooth, typically within about 10 metres. A **MAN (Metropolitan Area Network)** sits between LAN and WAN in scale, covering a city or

campus.

2 Network Hardware

For devices to communicate on a network, they need physical and electronic components. Each piece of hardware plays a specific role in getting data from one device to another.

Device	Full Name	What it does
NIC	Network Interface Card	Hardware that physically connects a device to a network (wired or wireless). Every networked device has one.
Hub	Network Hub	Sends data to **all** devices regardless of destination. Old, inefficient, rarely used today.
Switch	Network Switch	Sends data **only to the intended device** using MAC addresses. Standard in all modern networks.
Router	Network Router	Connects **different networks**; routes packets using IP addresses. Assigns local IPs via DHCP.
WAP	Wireless Access Point	Allows wireless devices to connect to a wired network. Usually built into home routers.
Modem	Modulator-Demodulator	Converts digital signals to analogue (and back) for transmission over phone lines. Needed for broadband access.
Firewall	Firewall	Monitors incoming/outgoing traffic and blocks unauthorised packets. Can be hardware or software.

2.1 Hubs vs Switches

When a hub receives a data packet, it **broadcasts** it to every connected device — like shouting a message in a crowded room hoping the right person hears it. This is wasteful; every device must process every packet, even ones not meant for them.

A switch is far more intelligent. It maintains a table of **MAC addresses** (unique hardware addresses) and sends each packet **only to the correct destination** — like handing someone a personalised letter. Switches dramatically reduce unnecessary traffic and are standard in all modern networks.

2.2 The Role of a Router

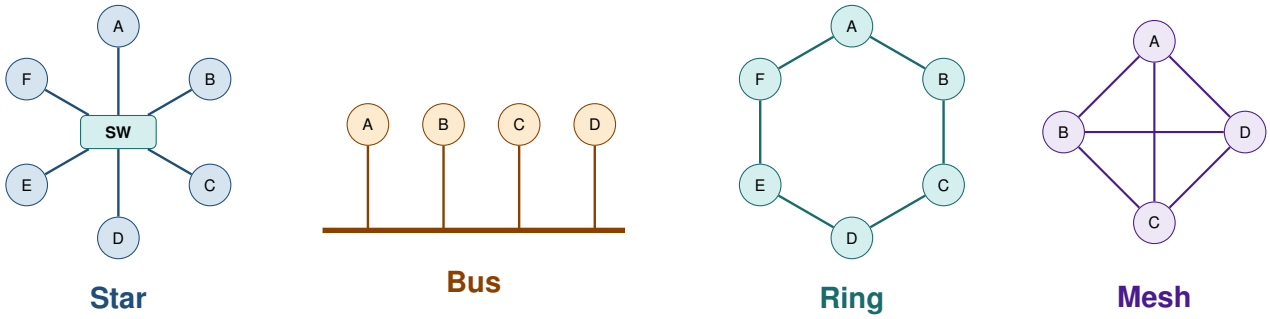
A router connects **different networks** together and decides the best path for data using **IP addresses**. Your home router connects your LAN to the internet (WAN). Most home

routers include a built-in switch, a wireless access point, and a DHCP server — so it is really several devices combined into one.

3 Network Topologies

A **network topology** describes how devices are physically or logically arranged and connected. Different topologies suit different contexts depending on cost, reliability, and scalability.

Topology	How it works	Advantages	Disadvantages
Star	All devices connect to a central switch or hub.	Easy to add devices; one cable fault only affects that device.	Central switch failure brings down the whole network.
Bus	All devices share one backbone cable.	Simple and cheap to install.	One break stops the entire network; collisions; poor scalability.
Ring	Devices in a loop; data travels one direction.	No collisions; equal access.	One failure disrupts the whole ring; hard to add/remove devices.
Mesh	Every device connects to every other (full) or some (partial).	Highly reliable; no single point of failure.	Expensive; very complex cabling.



3.1 Star Topology — The Industry Standard

The star topology is the most commonly used layout in modern networks. Every device connects directly to a central **switch**. Because each device has its own dedicated cable, a fault in one cable only affects **that single device** — the rest of the network continues working. The main weakness is the central switch: if it fails, the whole network loses connectivity. In practice, a good-quality managed switch is extremely reliable.

3.2 Bus Topology — Simple but Flawed

All devices share a single cable called the **backbone**. A single break anywhere in the backbone **takes down the entire network**. There is also a collision problem: if two devices transmit simultaneously, the signals interfere. Bus networks are rarely used today but remain examinable.

3.3 Ring Topology

Each device connects to exactly two others, forming a closed loop. Data travels in one direction, so there are no collisions. However, if any single device or connection fails, the entire network can be disrupted.

3.4 Mesh Topology — Most Reliable

In a full mesh every device connects to **every other device**, creating massive redundancy. For n devices, a full mesh requires $\frac{n(n-1)}{2}$ connections. In practice, **partial mesh** is used, where only the most critical nodes have multiple connections.

4 Wired vs Wireless Networks

	Wired (Ethernet)	Wireless (Wi-Fi)
Speed	Faster — up to 10 Gbps+	Slower; affected by interference and distance
Reliability	Very reliable; no interference	Affected by walls, devices, radio congestion
Security	More secure; physical access needed to intercept	Signals through air; easier to intercept without encryption
Mobility	Fixed to a cable port	High; devices move freely
Installation	Cables complex in large buildings	Easier; no cabling needed
Cost	Switches, cables, NICs add up	Access points cheaper across large areas

4.1 Types of Transmission Media

Copper (Ethernet) cables carry electrical signals and come in categories (Cat5e, Cat6, Cat6a) with increasing speed and shielding. They are cheap and easy to install.

Fibre-optic cables transmit data as pulses of **light**. This makes them much faster, immune to electromagnetic interference, and capable of carrying signals over very long distances without degradation. ISPs use them for the internet backbone.

Wireless (Wi-Fi) uses radio waves at **2.4 GHz** or **5 GHz**. The 2.4 GHz band has longer range but is more congested. The 5 GHz band is faster but struggles with walls. **Bluetooth** is a short-range standard designed for personal devices.

5 The Internet

The **internet** is a global network of networks — billions of devices connected using a common set of protocols. Do not confuse the internet with the **World Wide Web**: the web is just one service that *runs on* the internet. Email, online gaming, and video calls are also internet services but are not part of the web.

5.1 IP Addresses

Every device on a network is assigned an **IP address** — a unique numerical label used to identify it. Think of it like a postal address: you need it to send data to a specific device.

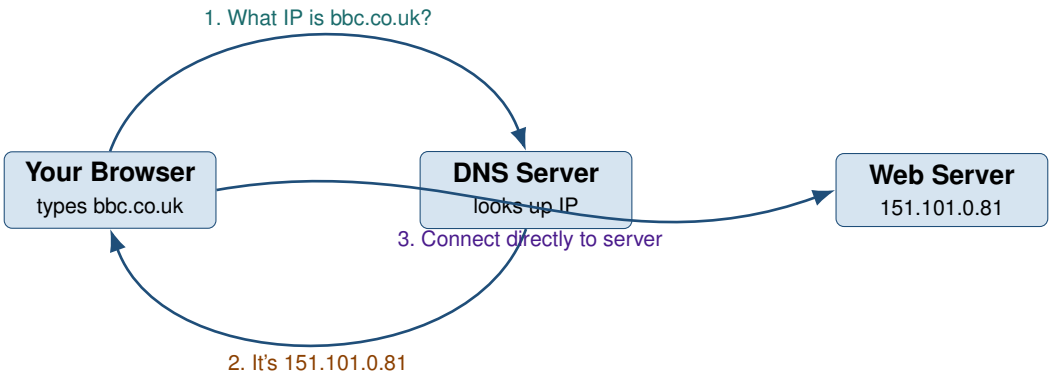
Feature	IPv4	IPv6
Bit length	32 bits	128 bits
Format	Four decimal numbers: `192.168.1.1`	Eight hex groups: `2001:0db8::8a2e:0370`
Total addresses	≈4.3 billion (now exhausted)	≈340 undecillion (essentially unlimited)
Notation	Dotted decimal	Colon-separated hexadecimal
Why needed?	Designed in the 1970s; address space has run out	Replaces IPv4 to solve the address shortage

5.2 Public vs Private IP Addresses

Your router has a **public IP address** visible to the internet, assigned by your ISP. Devices inside your home each have a **private IP address** (starting with `192.168.x.x` or `10.x.x.x`) assigned by the router via DHCP. When data leaves your network, the router uses **NAT (Network Address Translation)** to swap private IPs for the public one and track which internal device each reply belongs to.

5.3 DNS — The Internet's Phone Book

Humans find it easy to remember names like *www.bbc.co.uk*, but computers use numerical IP addresses. The **Domain Name System (DNS)** translates between the two. When you type a web address, your device queries a DNS server which replies with the correct IP address. Your device then connects directly to that IP.



5.4 Hosting and Cloud Computing

Websites run on **servers** — powerful computers that run continuously and respond to requests. **Cloud computing** takes this further: organisations rent computing resources over the internet from providers like Amazon (AWS), Microsoft (Azure), or Google, paying only for what they use and scaling instantly.

6 Network Protocols

A **protocol** is a set of rules governing how data is transmitted across a network. Without agreed protocols, devices made by different manufacturers could not communicate. Protocols define message format, error detection, how connections are opened and closed, and security.

6.1 Common Protocols

Protocol	Full Name	What it does	Port(s)
HTTP/HTTPS	HyperText Transfer Protocol (Secure)	Transfers web pages between browser and server. HTTPS adds TLS encryption.	80 / 443
FTP	File Transfer Protocol	Uploads and downloads files between client and server.	20/21
SMTP	Simple Mail Transfer Protocol	Sends email from client to mail server, or server to server.	25/587
IMAP/POP3	Internet Message Access / Post Office Protocol	IMAP reads email on the server (stays synced). POP3 downloads and deletes locally.	143 / 110
DNS	Domain Name System	Translates domain names into IP addresses.	53
DHCP	Dynamic Host Configuration Protocol	Automatically assigns IP addresses to devices joining a network.	67/68
SSH	Secure Shell	Provides encrypted remote terminal access to another computer.	22

6.2 TCP and UDP

Both are transport-layer protocols that move data between devices, but they take very different approaches.

TCP — Transmission Control Protocol	UDP — User Datagram Protocol
Connection-oriented: establishes a connection first via the three-way handshake (SYN, SYN-ACK, ACK).	**Connectionless:** fires packets immediately without establishing a connection.
Reliable: every packet is acknowledged; lost or corrupted packets are re-sent.	**Unreliable by design:** no acknowledgement; lost packets are simply not resent.
Ordered: packets are numbered and reassembled in the correct sequence.	**Fast:** skipping all checks gives much lower latency than TCP.
Use cases: web browsing, email, file downloads — where accuracy matters most.	**Use cases:** live video, online gaming, VoIP — where speed matters more than perfection.

Exam Tip: TCP vs UDP

TCP sacrifices speed to guarantee delivery; UDP sacrifices reliability to gain speed. A handy way to remember: losing a frame in a video call is barely noticeable, but losing

part of a bank transaction is a serious problem.

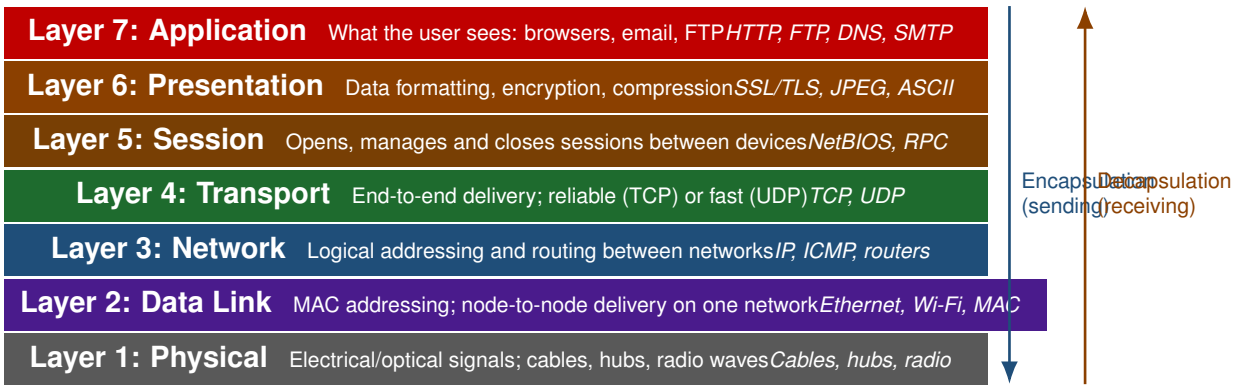
7 The OSI and TCP/IP Models

Layered models break network communication into separate, well-defined stages. Each layer has a specific job and passes data to the layer above or below it. This means that changes in one layer (e.g. switching from copper to fibre cable) do not require redesigning every other layer.

7.1 The OSI Model (7 Layers)

The **Open Systems Interconnection** model has 7 layers. Data travels **down** the layers on the sender (each layer adds a header — **encapsulation**) and **up** the layers on the receiver (each layer strips its header — **decapsulation**).

Mnemonic (top to bottom): "All People Seem To Need Data Processing"
Application, Presentation, Session, Transport, Network, Data Link, Physical



7.2 The TCP/IP Model (4 Layers)

The **TCP/IP model** is what the internet actually uses in practice. It is a simplified 4-layer model that combines several OSI layers.

Layer	Role	Examples
Application	Combines OSI layers 5–7; handles protocols applications use directly.	HTTP, FTP, DNS, SMTP
Transport	Reliable (TCP) or fast (UDP) delivery; manages port numbers.	TCP, UDP
Internet	IP addressing and routing across different networks.	IP, ICMP
Link	Physical hardware and local delivery. Combines OSI layers 1 and 2.	Ethernet, Wi-Fi

OSI vs TCP/IP

The OSI model is a theoretical framework used for teaching and troubleshooting. The TCP/IP model is the practical one used in real networks. For OCR GCSE you need to understand both, but TCP/IP and its protocols are more likely to appear in exam questions.

8 Network Security

Connecting to a network introduces security risks. Data can potentially be intercepted, modified, or misdirected, and unauthorised users may attempt to gain access. Understanding both threats and defences is a core part of this topic.

8.1 Common Threats

8.1.1 Malware

Malware (malicious software) is any software designed to harm a system or steal data.

- **Viruses:** attach to legitimate files and spread when those files are shared.
- **Worms:** self-replicating; spread across networks without any user action.
- **Trojans:** disguised as legitimate software; secretly give attackers access.
- **Ransomware:** encrypts the victim's files and demands payment for the decryption key.
- **Spyware:** silently monitors user activity and sends data to attackers.

8.1.2 Phishing

Phishing is a **social engineering** attack where a cybercriminal sends a deceptive message (usually an email) pretending to be a trusted organisation such as a bank. The goal is to trick the user into revealing sensitive information or clicking a link that installs malware. **Spear phishing** is a targeted version using personal details to make the message more convincing.

8.1.3 Denial of Service (DoS) and DDoS

A **DoS attack** floods a server with so many requests it becomes overwhelmed and unable to serve legitimate users. A **DDoS attack** (Distributed DoS) uses thousands of compromised machines (a **botnet**) simultaneously, making it much harder to block. Online services, gaming platforms, and banks are common targets.

8.1.4 Man-in-the-Middle (MitM)

An attacker secretly intercepts and potentially alters communication between two parties who believe they are communicating only with each other. On unsecured Wi-Fi, an attacker on the same network can intercept unencrypted traffic.

8.1.5 SQL Injection

An attacker types malicious SQL code into an input field (such as a login form) hoping the server will execute it as a database command. A successful attack can bypass logins, extract passwords, or delete the entire database. The defence is **sanitising user input** — always treating input as plain text, never as executable code.

8.2 Security Measures

8.2.1 Firewalls

A firewall monitors all incoming and outgoing traffic and blocks anything that violates its rules (based on IP address, port, or protocol). A **hardware firewall** is a dedicated device at the network boundary; a **software firewall** runs on an individual device. Most organisations use both.

8.2.2 Encryption

Encryption converts data into a coded form readable only with the correct key.

Type	How it works	Key properties
Symmetric	The **same key** both encrypts and decrypts. Both parties must have it.	Fast; challenge: how do you share the key securely?
Asymmetric	A **key pair**: a public key (shared openly) and a private key (kept secret). Data encrypted with the public key can only be decrypted with the private key.	Slower; solves the key-sharing problem; used in HTTPS/TLS.

When you visit an **HTTPS** website, **TLS (Transport Layer Security)** uses asymmetric encryption to securely exchange a symmetric key, then switches to symmetric encryption for the session (because it is faster). This is why the padlock appears in your browser's address bar.

8.2.3 Authentication and Access Control

Multi-factor authentication (MFA) requires two or more types of evidence: something you *know* (password), something you *have* (authenticator app), or something you *are* (fingerprint). **Access control lists (ACLs)** define precisely what each authenticated user or device is permitted to do.

8.2.4 MAC Address Filtering

Access points can be configured to only accept devices whose MAC addresses are on an approved list. Not foolproof (MAC addresses can be *spoofed*), but a useful extra layer.

> **Defence in Depth**
>
> No single measure is sufficient on its own. Layering firewall + encryption + MFA + access controls means that if one fails, others are still protecting the system.

9 Client-Server and Peer-to-Peer Networks

9.1 Client-Server Architecture

Servers are powerful computers dedicated to providing services. **Clients** are the devices used by people. When you log in to a school network, your laptop authenticates against a

server; files are fetched from a file server; printing goes to a print server.

Advantages	Disadvantages
Centralised management — files, users, and permissions controlled from one place.	Expensive to set up; specialist IT staff required.
Easy to apply security policies and software updates across all clients.	If the server fails, all clients lose access to files and services.
Data backed up centrally, reducing risk of data loss.	Requires ongoing maintenance by trained IT staff.

9.2 Peer-to-Peer (P2P) Architecture

There is no dedicated server. Every device acts as **both client and server**, sharing its own files directly with any other device. P2P is common in homes and applications like BitTorrent.

Advantages	Disadvantages
Much cheaper — no dedicated server hardware needed.	Difficult to manage centrally or enforce security policies.
No single point of failure; if one device goes offline, others continue.	Performance drops when a device is sharing resources with others.
Simple to configure for small home networks.	No centralised backup; scales poorly with many devices.

10 Bandwidth, Latency and Packet Switching

10.1 Bandwidth and Latency

Bandwidth	Latency
The **maximum volume of data** transmittable per second. Measured in Mbps or Gbps. Think of it as the *width* of a pipe — wider means more data at once. Critical for 4K streaming, large file transfers, and many simultaneous users.	The **time delay** between sending data and it arriving. Measured in milliseconds (ms). Think of it as the *length* of a pipe — even a wide pipe takes time if it is very long. Critical for gaming, video calls, and financial trading.

10.2 Packet Switching

Data is broken into small chunks called **packets**, each containing the payload plus a **header** (addresses, sequence number, etc.). Packets from the same message can take **different routes** across the network, whichever is least congested. Routers make these routing decisions in real time. On arrival, packets are reassembled in order (TCP handles this). Multiple communications can share the same physical links simultaneously, making the network highly efficient.

What's inside a packet?

- **Source IP address:** where the packet came from.
- **Destination IP address:** where the packet is going.
- **Sequence number:** for reassembling packets in the correct order.
- **Time to Live (TTL):** limits hops before the packet is discarded; prevents infinite loops.
- **Data payload:** the actual chunk of content (typically up to ≈1,500 bytes on Ethernet).
- **Checksum:** a calculated value for detecting transmission errors.

11 VLANs and Cloud Computing

11.1 VLANs

A **VLAN (Virtual Local Area Network)** creates separate, logically isolated networks on the same physical hardware. In a school, staff and student networks share the same switches and cables but remain completely separate via VLAN configuration. VLANs improve both **security** and **performance** (by reducing unnecessary broadcast traffic).

11.2 Cloud Computing

Organisations rent computing resources (servers, storage, software) over the internet from providers like Amazon AWS, Microsoft Azure, or Google Cloud, rather than buying and maintaining their own hardware.

Advantages	Disadvantages
Scalable — instantly increase or decrease resources.	Requires reliable internet; no internet = no access.
Lower upfront cost; no server hardware to buy.	Ongoing costs can exceed one-time hardware costs over time.
Accessible from anywhere with internet.	Data on third-party servers raises privacy and security concerns.
Provider handles hardware maintenance and updates.	Vendor lock-in: difficult to switch providers once embedded.
Automatic backups and disaster recovery included.	Less control over data location (may be in another country).

12 Key Terms Glossary

Term	Definition
Bandwidth	The maximum volume of data a network can transmit per second (Mbps/Gbps).
Checksum	A value calculated from data used to detect errors in transmission.
Client	A device that requests services from a server.
DHCP	Protocol that automatically assigns IP addresses to devices on a network.
DNS	System translating domain names into IP addresses.
Encryption	Converting data into a coded form so only authorised recipients can read it.
Firewall	Hardware/software that monitors and controls network traffic using defined rules.
FTP	Protocol for transferring files between a client and a server.
HTTP/HTTPS	Protocol for transferring web pages; HTTPS adds TLS encryption.
IP address	A unique numerical address assigned to each device on a network.
IPv4	32-bit IP addressing scheme with ≈4.3 billion addresses.
IPv6	128-bit scheme replacing IPv4 due to address exhaustion.
LAN	Local Area Network — confined to one site or building.
Latency	The time delay in transmitting data across a network.
MAC address	A unique hardware address assigned to every network interface card.
Malware	Malicious software designed to damage systems or steal data.
NIC	Network Interface Card — physically connects a device to a network.
OSI model	A 7-layer theoretical framework for understanding network communication.
Packet	A small chunk of data plus a header, sent independently across a network.
Packet switching	Breaking data into packets and routing each independently across a network.
Phishing	A social engineering attack tricking users into revealing sensitive information.
Protocol	A set of rules governing how data is transmitted between devices.
Router	Connects different networks; routes packets between them using IP addresses.
Server	A powerful computer that provides services and resources to clients.
SMTP	Protocol for sending email.
SQL injection	Attack inserting malicious SQL code into a website's database query.
SSL/TLS	Protocols that encrypt data in transit; used in HTTPS.

If you find any mistakes email me at dennis.mihailov.dm@gmail.com — OCR GCSE Computer Science: Networks