# Networks

IB SL Study Guide

---

## Contents

# Network Types

A **computer network** is a collection of devices connected together to share resources and communicate. Networks are classified by their geographic scale and ownership.

## LAN, WAN, and WLAN

| Type | Full Name | Coverage | Ownership | Typical Speed |
|---|---|---|---|---|
| **LAN** | Local Area Network | Single building or campus | Private (owned by the organisation) | High (100 Mbps – 10 Gbps) |
| **WAN** | Wide Area Network | City, country, or global | Public/leased (ISPs, telecoms) | Variable (slower than LAN) |
| **WLAN** | Wireless LAN | Same as LAN but wireless | Private | Moderate (up to ~600 Mbps via Wi-Fi) |

The **internet** is the largest WAN — a global network of interconnected networks using standardised protocols.

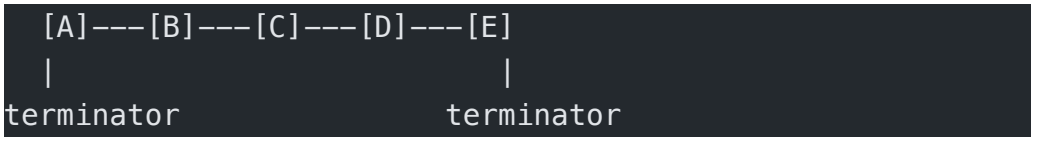
> **IB TIP**
>
> When comparing LAN and WAN in an exam, address: coverage (geographic scale), ownership (private vs. public/leased), and typical speed. These three attributes map directly to mark schemes. Avoid saying "LAN is faster" without explaining why — it is faster because it uses dedicated private cabling over shorter distances.

# Network Topologies

A **network topology** describes how devices (nodes) are physically or logically connected. The three topologies tested in IB CS SL are bus, star, and ring.

## Bus Topology

All devices connect to a single shared cable (the **bus**). Data travels in both directions along the bus; terminators at each end absorb signals to prevent reflection.




| Pros | Cons |
|---|---|
| Simple and cheap to install | A break anywhere in the cable takes down the whole network |
| Requires less cable than star | Performance degrades as more devices are added (collisions) |
| Easy to extend | Difficult to troubleshoot |

### Star Topology

All devices connect to a central switch or hub. Data passes through the central device to reach its destination.


| Pros | Cons |
|---|---|
| A cable failure only affects one device | If the central switch fails, the entire network goes down |
| Easy to add or remove devices | Requires more cable than bus |
| Easier to diagnose faults | Switch is a single point of failure |
| Better performance under heavy traffic (dedicated connections via switch) | |

### Ring Topology

Devices are connected in a closed loop. Data travels in one direction (or both in dual-ring) around the ring; each device acts as a repeater.


| Pros | Cons |
|---|---|
| No data collisions (token passing controls access) | A break in the ring can take down the network (unless dual-ring) |
| Performance is predictable | Adding or removing devices disrupts the network |
| Signals can be regenerated at each node | More complex to manage than bus |

**MEMORISE THIS**

**Topology trade-offs summary:**

- **Bus** — cheapest, highest risk (one break = all down)
- **Star** — most common, single point of failure at the switch
- **Ring** — orderly but fragile; rare in modern networks

**EXAM ALERT**

The most common exam mistake on topologies is stating that a star topology fails if "one cable breaks". A cable break in a star only affects the single device on that cable. The failure point is the **central switch or hub**, not a cable. State this clearly.

# Network Hardware

Understanding the role of each hardware component is essential for Paper 1 questions.

### Devices and Their Roles

| Device | Role |
|---|---|
| **Router** | Connects different networks (e.g., LAN to the internet); forwards packets between networks using IP addresses; assigns local IP addresses via DHCP |
| **Switch** | Connects devices within a LAN; sends data only to the specific destination device using MAC addresses (unlike a hub) |
| **Hub** | Connects devices in a LAN; broadcasts all data to every connected device regardless of destination (inefficient; largely obsolete) |
| **Access Point (AP)** | Extends a wired LAN wirelessly; devices connect via Wi-Fi to the AP, which connects to the network via Ethernet |
| **NIC** | Network Interface Card — hardware inside each device that enables it to connect to a network; has a unique MAC address burned in at manufacture |
| **Modem** | Modulates/demodulates signals to convert digital data to/from analogue signals for transmission over telephone or cable lines; used to connect to an ISP |

> **IB TIP**
>
> Distinguish switch from hub: a **switch** uses MAC address tables to send data only to the correct port (unicast), so only the destination device receives it. A **hub** broadcasts to all ports, wasting bandwidth and creating security concerns. IB questions frequently use the word “hub” when they mean “switch” — read carefully and use precise terms.

# Protocols

A **protocol** is a set of agreed rules that govern how data is transmitted between devices on a network. Without common protocols, devices from different manufacturers could not communicate.

### Key Protocols Table

| Protocol | Full Name | Purpose |
|---|---|---|
| **HTTP** | HyperText Transfer Protocol | Transfers web pages between server and browser (unencrypted) |
| **HTTPS** | HTTP Secure | Same as HTTP but with TLS/SSL encryption — data cannot be read by third parties |
| **TCP** | Transmission Control Protocol | Reliable, connection-oriented transport; guarantees delivery, ordering, and error checking via acknowledgements |
| **IP** | Internet Protocol | Addressing and routing packets across networks using IP addresses |
| **DNS** | Domain Name System | Translates human-readable domain names (e.g., `studyforge.com`) into IP addresses |
| **DHCP** | Dynamic Host Configuration Protocol | Automatically assigns IP addresses, subnet masks, and gateway addresses to devices joining a network |

### TCP/IP Four-Layer Model

The **TCP/IP model** (also called the Internet model) describes how data is processed as it moves from application to physical network and back.

| Layer | Name | Responsibility | Example Protocols |
|---|---|---|---|
| 4 | Application | Provides network services to end-user applications | HTTP, HTTPS, DNS, DHCP, FTP, SMTP |
| 3 | Transport | End-to-end communication; segmentation, reliability, flow control | TCP, UDP |
| 2 | Internet | Logical addressing and routing of packets between networks | IP |
| 1 | Network Access (Link) | Physical transmission of data over the local network medium | Ethernet, Wi-Fi (IEEE 802.11) |

When data is sent, each layer **encapsulates** the data from the layer above by adding its own header. On the receiving side, each layer **decapsulates** (removes the header) and passes the data up.

> ⚠ **EXAM ALERT**
>
> IB examiners sometimes ask which layer DNS or DHCP operates at. Both are **Application layer** protocols, even though they support network infrastructure functions — they are accessed by applications and use TCP or UDP at the Transport layer.

## IP Addressing

Every device on a network requires a unique **IP address** to send and receive data. IP addressing provides the logical addressing that enables routing across networks.

### IPv4

IPv4 addresses are 32-bit values written as four decimal octets separated by dots, for example: `192.168.1.105`

Each octet represents 8 bits, with a value from 0 to 255.

- **Network portion** — identifies the network (determined by the subnet mask)
- **Host portion** — identifies the specific device on that network

**Total possible IPv4 addresses:** $2^{32} \approx 4.3$ billion — this is now insufficient for the global internet, which is why IPv6 was developed.

### Subnet Basics

A **subnet mask** (e.g., `255.255.255.0`) indicates which bits of the IP address identify the network and which identify the host. Devices on the same subnet can communicate directly; devices on different subnets communicate via a router.

### IPv6

IPv6 addresses are 128-bit values written in eight groups of four hexadecimal digits, for example: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`

IPv6 provides $2^{128}$ possible addresses — effectively unlimited for the foreseeable future. IPv6 also includes built-in security features and simplified routing.

> **IB TIP**
>
> For IB SL you need to know: IPv4 is 32-bit, dotted decimal notation, approximately 4.3 billion addresses; IPv6 is 128-bit, hexadecimal notation, created to solve IPv4 address exhaustion. You are not required to perform subnetting calculations.

## Client-Server vs Peer-to-Peer

Networks can be organised around two fundamental architectures.

### Client-Server

A **server** provides services or resources; **clients** request and consume them.

- Server is a dedicated, always-on machine with high performance
- Centralised management: data, security, and backups controlled from one point
- Scales well: many clients can share server resources
- Single point of failure: if the server goes down, clients lose access

**Examples:** web servers (HTTP), email servers (SMTP), file servers, authentication servers (Active Directory)

### Peer-to-Peer (P2P)

All devices are equal (**peers**) and can act as both client and server simultaneously.

- No dedicated server: each device shares its own resources directly
- Decentralised: no single point of failure
- Cheap to set up: no server hardware required
- Harder to manage: security, backups, and permissions must be configured on each device
- Performance degrades as load increases on individual devices

**Examples:** BitTorrent file sharing, some online gaming networks, older home networks

| Attribute | Client-Server | Peer-to-Peer |
|---|---|---|
| Management | Centralised | Distributed (each peer) |
| Cost | High (server hardware) | Low |
| Security | Easier to control | Harder to enforce uniformly |
| Reliability | Depends on server uptime | No single point of failure |
| Scalability | High | Limited by individual peer capacity |

## Data Transmission and Packet Switching

Rather than sending data as a continuous stream, the internet breaks data into small units called **packets**.

### Packet Switching

In **packet switching**, each packet is routed independently across the network and may take different paths to reach the destination. Packets are reassembled in the correct order at the destination.

**Advantages of packet switching:**

- Network resources are used efficiently (no dedicated line needed for each conversation)
- If one path fails, packets are rerouted automatically
- Multiple conversations can share the same links simultaneously

### Packet Structure

Each packet contains three sections:

| Section | Contents |
|---|---|
| **Header** | Source IP address, destination IP address, sequence number, protocol, TTL (time to live) |
| **Payload** | The actual data being transmitted (a chunk of the file, web page, etc.) |
| **Trailer** | Error-checking information (checksum); some protocols omit the trailer |

### Bandwidth vs Latency

| Term | Definition | Analogy |
|---|---|---|
| **Bandwidth** | The maximum amount of data that can be transmitted per second (Mbps or Gbps) | Width of a pipe |
| **Latency** | The time delay for a packet to travel from source to destination (milliseconds) | Length of the pipe |

High bandwidth but high latency = large files transfer quickly overall, but each request takes time to begin. Low latency is critical for real-time applications (video calls, online gaming).

## Network Security

Protecting networks from threats is a core syllabus area. Students must know both the types of threats and the corresponding protective measures.

### Common Threats

| Threat | Description |
|---|---|
| **Malware** | Malicious software including viruses (self-replicating, attach to files), worms (self-replicating, spread via network), ransomware (encrypts user data, demands payment), trojans (disguised as legitimate software) |
| **Phishing** | Deceptive emails or websites that trick users into revealing passwords or financial information |
| **Denial of Service (DoS)** | Flooding a server with traffic to make it unavailable to legitimate users; DDoS uses many compromised machines simultaneously |
| **Man-in-the-Middle (MitM)** | An attacker intercepts and potentially alters communication between two parties without their knowledge |
| **SQL Injection** | Malicious SQL code inserted into input fields to manipulate a database |
| **Social Engineering** | Manipulating people (rather than systems) into revealing confidential information |

### Protective Measures

| Protection | How It Helps |
|---|---|
| **Firewall** | Monitors and filters incoming/outgoing network traffic based on rules; blocks unauthorised access |
| **Encryption** | Transforms data into an unreadable ciphertext; only parties with the correct key can decrypt it — protects data in transit and at rest |
| **HTTPS / TLS** | Encrypts all data between the browser and web server using TLS; prevents MitM interception of web traffic |
| **VPN** | Virtual Private Network — creates an encrypted tunnel between the user and a remote server, hiding traffic from ISPs and local eavesdroppers |
| **Two-Factor Authentication (2FA)** | Requires a second verification step (e.g., code sent to phone) in addition to a password — protects against stolen passwords |
| **Antivirus / Anti-malware** | Detects and removes known malware signatures; monitors for suspicious behaviour |
| **Regular software updates** | Patches known security vulnerabilities that attackers could exploit |

⚠ EXAM ALERT

IB Paper 1 frequently asks "identify one threat and one corresponding protection". Match them precisely: phishing → user education and 2FA; DoS → firewall and traffic filtering; MitM on public Wi-Fi → VPN and HTTPS. A protection that doesn't address the specific threat described will not receive marks.

MEMORISE THIS

**Threat–Protection pairings to memorise:**

- Stolen password → 2FA
- Unencrypted data in transit → HTTPS/VPN
- Unauthorised network access → Firewall
- Malware download → Antivirus + user education
- Phishing link clicked → User training + email filtering

## Practice Questions

▶ Q1 — Describe the role of a router on a home network. [3 marks]

▶ Q2 — Explain one advantage and one disadvantage of a star topology compared to a bus topology. [4 marks]

▶ Q3 — State the purpose of DNS and explain what happens when a user types a web address into their browser. [4 marks]

▶ Q4 — A student uses public Wi-Fi in a café to access their online banking. Identify two security risks and suggest one protective measure for each. [4 marks]

▶ Q5 — Explain the difference between bandwidth and latency. Give one situation where each matters more than the other. [4 marks]

▶ Q6 — State the difference between a DoS attack and a DDoS attack and explain why DDoS is harder to defend against. [3 marks]